



***Common Criteria***  
**Evaluation and Validation Scheme**  
for  
Information Technology Security

**Organization, Management and Concept of Operations**

Scheme Publication #1

Version 2.0

May 1999

National Institute of Standards and Technology  
Information Technology Laboratory  
100 Bureau Drive  
Gaithersburg, MD 20899

National Security Agency  
Information Systems Security Organization  
9800 Savage Road  
Fort George G. Meade, MD 20755



## Table of Contents

1	Introduction .....	1
1.1	Objectives .....	1
1.2	IT Security Evaluation and Validation.....	2
1.3	Historical Perspective .....	3
1.4	Organization of this Document.....	3
1.5	Scheme Publications .....	4
2	Overview of the Scheme.....	5
3	Roles and Responsibilities.....	8
3.1	Sponsor of an IT Security Evaluation .....	8
3.2	NIAP Validation Body .....	8
3.3	Common Criteria Testing Laboratories.....	10
3.4	Guidance for Consumers .....	11
4	IT Security Evaluation.....	13
4.1	Preparation for IT Security Evaluation.....	13
4.2	Conduct of the IT Security Evaluation .....	15
4.3	Conclusion of the Evaluation.....	16
4.4	Evaluation of Protection Profiles .....	17
5	Technical Oversight and Validation .....	19
5.1	Technical Oversight.....	19
5.2	The Validation Process .....	20
5.3	Common Criteria Certificates .....	21
	References.....	23
	Acronym List .....	25
	Publications List .....	26
	Annex A. Glossary.....	27
	Annex B. Requirements for Validation Body .....	31
	Annex C. Requirements for Testing Laboratories .....	34
	Annex D. Responsibilities of Evaluation Sponsors.....	38
	Annex E. Common Criteria Certificates.....	41
	Annex F. Certificate Maintenance.....	44
	Annex G. Demonstrating Common Criteria Conformance.....	49
	Annex H. Letter of Intent.....	51

# 1 Introduction

Recent advances in information technologies and the proliferation of computing systems and networks world wide have raised the level of concern about security in both the public and private sectors. This concern has been reinforced in the final report of President's Commission on Critical Infrastructure Protection [CIP97] and the associated Presidential Decision Directive 63 (PDD-63) [CIP98]. Security concerns are motivated by an increasing use of information technology (IT) *products* and *systems* throughout government and industry in a variety of areas—from electronic commerce to national defense. Consumers have access to a growing number of security-enhanced IT products with different capabilities and limitations and must make important decisions about which products provide an appropriate degree of protection for their information.

In order to help consumers select commercial off-the-shelf IT products<sup>1</sup> that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace, the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have established a program under the National Information Assurance Partnership (NIAP)<sup>2</sup> to evaluate IT product conformance to international standards. The program, officially known as the *NIAP Common Criteria Evaluation and Validation Scheme for IT Security*, (or Common Criteria Scheme in abbreviated form), is a partnership between the public and private sectors.

## 1.1 Objectives

NIST and NSA have the following objectives in developing, operating, and maintaining an evaluation and validation scheme:

- a) to meet the needs of government and industry for cost-effective evaluation of IT products;
- b) to encourage the formation of commercial security testing laboratories and the development of a private sector security testing industry;
- c) to ensure that security evaluations of IT products are performed to consistent standards;
- d) to improve the availability of evaluated IT products.

The scheme is intended to serve many communities of interest with very diverse roles and responsibilities. This community includes IT product developers, product vendors, value-added resellers, systems integrators, IT security researchers, acquisition/procurement authorities, consumers of IT products, auditors, and accreditors (individuals deciding the fitness for operation of those products within their respective organizations). Close cooperation between government and industry is paramount to the success of the scheme and the realization of its objectives.

---

<sup>1</sup> The Common Criteria Scheme employs a relatively broad definition of IT product. That is, an IT product can be a single product or multiple products configured as an IT system or system solution to meet certain consumer needs. In either case, the evaluation is conducted in a security testing facility under laboratory conditions and not in actual operational environments.

<sup>2</sup> The National Information Assurance Partnership (NIAP) is a joint NIST-NSA initiative designed to meet the security testing needs of both IT producers and consumers. The partnership is intended to foster the availability of objective measures and test methods for evaluating the quality of IT security products. In addition, it is designed to foster the development of commercial testing laboratories that can provide the types of security testing and evaluation services which will meet the demands of both producers of IT products and consumers of those products.

## 1.2 IT Security Evaluation and Validation

IT security is defined as the protection of information from unauthorized disclosure, modification, or loss of use by countering threats to that information arising from human or systems-generated activities, malicious or otherwise. Countering threats to an IT product and mitigating risk helps to protect the confidentiality and integrity of information and also ensure its availability.

Consumers of IT products need to have confidence in the security features of those products. Consumers want to be able to compare various products to understand their capabilities and limitations. Confidence in a particular IT product can be based on the trusted reputation of the developer, past experience in dealing with the developer, or the demonstrated competence of the developer in building products through recognized assessments. The consumer could also test the product directly and obtain the necessary results. The first approach lacks measurable results and the second approach requires substantial, costly duplication of effort.

The Common Criteria Scheme will overcome these limitations and enable consumers to obtain an impartial assessment of an IT product by an independent entity. This impartial assessment, or *security evaluation*, includes an analysis of the IT product and the testing of the product for conformance to a set of security requirements. The specific IT product being evaluated is referred to as the *Target of Evaluation (TOE)*. The security requirements for that product are described in its *security target*.<sup>3</sup> IT security evaluations are composed of analysis and testing, distinguishing these activities from the more traditional forms of conformance testing in other areas.

It is important that security evaluations of IT products be carried out in accordance with recognized standards and procedures. The use of standard IT security evaluation criteria and IT security evaluation methodology<sup>4</sup> contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgement and background knowledge for which consistency is more difficult to achieve.

To increase the consumer's level of confidence in IT security evaluations, the final evaluation results can be reviewed by an independent party. This review provides independent confirmation that an IT security evaluation has been conducted in accordance with the provisions of the scheme and that the conclusions of the testing laboratory are consistent with the facts presented in the evaluation. This review, known as *validation*, is intended to promote consistency of IT security evaluations and comparability of results for all evaluations conducted within the scheme.

The impartial evaluation, the independent validation of evaluation results, and the documentation resulting from these processes provide valuable information for consumers about the security capability of IT products. However, consumers will still need to review this information carefully and assess its applicability to local needs, (e.g., the situation and operating environment in which the product will actually be used). Section 3.4 of this document provides additional guidance to consumers of IT products regarding the specific use of security evaluation results.

Participation in the scheme and its associated evaluation and validation activities is strictly voluntary (unless mandated by government policy or regulation). In addition, organizations may undertake alternative activities to use the Common Criteria and to demonstrate product conformance to IT security requirements. While these activities are recognized as legitimate for certain constituencies or communities of interest, they are outside the scope of the scheme as

---

<sup>3</sup> The Common Criteria provides constructs for stating security requirements that support developers in identifying those requirements to be satisfied by their product. The developers can use those constructs to make claims that their product, (i.e., Target of Evaluation) conforms to those requirements by means of specified security functions and assurances to be evaluated. These requirements are contained in an implementation-dependent construct called a *security target*.

<sup>4</sup> The *Common Criteria for IT Security Evaluation* [COM98] and the *Common Methodology for IT Security Evaluation* [CEM99] will be used as the standard evaluation criteria and evaluation methodology, respectively, for all security evaluations of IT products within the scheme. The Common Criteria is an international standard (ISO/IEC 15408).

described in this document. A more complete description of these testing and evaluation activities and how these activities relate to the scheme can be found in Annex G.

### **1.3 Historical Perspective**

The U.S. Government supports the security and trustworthiness of IT products that are part of the national information infrastructure, both in the public and private sectors. In fulfilling their responsibilities under Public Law 100-235 (Computer Security Act of 1987), NIST and NSA have worked with government and industry to develop and apply information security technology, assurance metrics and standards necessary for the protection of information critical to the overall economic and national security interests of the United States.

For over two decades, NIST and NSA have promoted security in commercial off-the-shelf IT products. These efforts have focused primarily on government-sponsored initiatives to produce effective IT security evaluation criteria, (e.g., the *Trusted Computer System Evaluation Criteria* [DOD85] and the *Federal Criteria for Information Technology Security* [FED92]), and to evaluate products developed by industry in response to those criteria. The development of similar IT security evaluation criteria by Canada and several European nations during the last decade and recognition of the increasing world wide markets for U.S. manufacturers of IT products, prompted the effort to begin harmonizing existing evaluation criteria into common criteria—internationally-accepted and standards based. The Common Criteria is the result of a multi-year effort by the governments of the U.S., Canada, United Kingdom, France, Germany, and the Netherlands to develop a harmonized security criteria for IT products.

At the same time the Common Criteria were being developed, there was a parallel effort to transition trusted product evaluations from the government to the private sector. NSA began the transition of its commercial IT product evaluation capability, (i.e., the Trusted Product Evaluation Program) to the private sector with the establishment of the Trust Technology Assessment Program (TTAP).<sup>5</sup> Under this program, IT security evaluations are conducted by commercial testing laboratories using the current NSA evaluation methodology in accordance with cooperative research and development agreements. The transition will continue under the Common Criteria Scheme with commercial testing laboratories conducting Common Criteria-based evaluations of IT products on a fee-for-service basis using the Common Methodology.

### **1.4 Organization of this Document**

This document consists of five chapters and several supporting annexes. Chapter 1 introduces the concept of an evaluation and validation scheme; its purpose, scope and historical perspective. Chapter 2 provides a general overview of the scheme and a brief description of its major activities. Chapter 3 defines the roles and responsibilities of the key participants in the scheme to include the NIAP Validation Body, Common Criteria Testing Laboratories, and sponsors of IT security evaluations. Chapter 4 describes the activities associated with conducting IT security evaluations. Chapter 5 elaborates on the concept of technical oversight and validation and describes the interaction between the Validation Body and security testing laboratories.

The supporting annexes cover a variety of topics to include requirements for the NIAP Validation Body, procedures for establishing accredited testing laboratories, obligations of sponsors of IT security evaluations, the form and content of Common Criteria certificates, and the scheme approach for maintaining the currency of IT security evaluation results in an environment of

---

<sup>5</sup> Commercial testing laboratories operating under the TTAP or any other IT security evaluation program will not be automatically admitted into the Common Criteria Scheme, (i.e., grandfathered into the scheme). Testing laboratories desiring to conduct Common Criteria-based evaluations within the scheme will be required to seek admission to the scheme in accordance with the policies and procedures outlined in this document without regard to their previous status.

rapidly changing product and system technologies. There is also a glossary of terms related to criteria, methodology, evaluation, accreditation of testing laboratories, and the scheme.

## **1.5 Scheme Publications**

The NIAP Validation Body will communicate to sponsors of evaluations, testing laboratories, government agencies, and the general public through a series of technical and administrative publications. The flagship document in the series is Scheme Publication #1, *Common Criteria Evaluation and Validation Scheme for IT Security—Organization, Management, and Concept of Operations*. Subsequent publications will provide guidance to sponsors of IT security evaluations, guidance to security testing laboratories, guidance on evaluating specific information technologies, guidance on employing and interpreting the Common Criteria and Common Methodology, and guidance on protection profile and security target development. Additional information and guidance will be available on other important scheme topics such as technical oversight, validation, Common Criteria certificates and certificate maintenance. These publications will be updated as needed to maintain currency. Copies of all scheme publications and other important information about the NIAP Validation Body, commercial testing laboratories, and validated IT products will be available on the NIAP web site at <http://niap.nist.gov>.

## 2 Overview of the Scheme

This chapter provides a general overview of the Common Criteria Scheme. The principal participants in the scheme are:

- a) Sponsors of IT security evaluations;
- b) NIAP Validation Body (NIST/NSA);
- c) Common Criteria Testing Laboratories.

In addition to the principal participants listed above, NIST's *National Voluntary Laboratory Accreditation Program (NVLAP)* plays an important role in supporting the scheme requirements for laboratory accreditation.

In the context of the Common Criteria Scheme, a sponsor is the party requesting and paying for the security evaluation of an IT product or *protection profile*<sup>6</sup> by an accredited testing laboratory. The sponsor is often the product or profile developer, but could also be a government agency, industry consortium, or other organization seeking to obtain an IT security evaluation.

The NIAP Validation Body is an activity jointly managed by NIST and NSA and staffed by technical/administrative personnel from those agencies. Operating in the interest of the public and private sectors, the Validation Body approves participation of security testing laboratories in the scheme in accordance with its established policies and procedures. It also provides technical guidance to those testing laboratories, validates the results of IT security evaluations for conformance to the Common Criteria, and serves as an interface to other nations on the recognition of such evaluations. Specific requirements for the Validation Body are described in Annex B.

IT security evaluations are conducted by commercial testing laboratories accredited by NVLAP and *approved* by the NIAP Validation Body. These approved testing laboratories are called Common Criteria Testing Laboratories (CCTL). NVLAP accreditation is the primary requirement for becoming a CCTL.<sup>7</sup> The purpose of the NVLAP accreditation is to ensure that laboratories meet the requirements of ISO/IEC Guide 25, *General Requirements for the Competence of Calibration and Testing Laboratories* [ISO90] and the specific scheme requirements for IT security evaluations.

---

<sup>6</sup> A protection profile is a Common Criteria construct that defines an implementation-independent set of IT security requirements (both features and assurances) for a category of IT products. Such generalized requirements are intended to meet common needs for IT security. Consumers can therefore, construct or cite a protection profile to express their IT security needs without reference to any specific IT product. Sponsors may employ CCTLs to formally evaluate protection profiles in accordance with the Common Criteria and the Common Methodology. The results of such evaluations can be validated by the NIAP Validation Body and appropriate Common Criteria certificates issued. Protection profiles can subsequently be listed in a special section of the validated products list.

<sup>7</sup> At the present time, NVLAP accreditation is both the necessary and sufficient condition to receiving NIAP approval to become a CCTL. If, however, there are subsequent scheme requirements in the future that cannot be addressed solely by NVLAP accreditation, those requirements will be handled by the NIAP Validation Body as part of the overall laboratory approval process. These additional requirements will be described in Scheme Publication #2, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Validation Body Standard Operating Procedures*.



With respect to NVLAP, the scope of accreditation is defined to be the particular *test methods*<sup>8</sup> that a laboratory will use in conducting IT security evaluations. A testing laboratory will choose its scope of accreditation from a list of approved test methods developed by the NIAP Validation Body. The Validation Body maintains a *NIAP Approved Test Methods List* for use by a laboratory in selecting its proposed scope of accreditation. The Validation Body will coordinate with NVLAP to assure that appropriate accreditation is made available to CCTLs. Once NVLAP accreditation is received and any additional scheme-specific requirements are met, the CCTL will be placed on the *NIAP Approved Laboratories List*.

CCTLs wishing to expand their scope of accreditation, (i.e., adding new test methods), will coordinate with NVLAP and the NIAP Validation Body. Specific details regarding NVLAP accreditation, re-accreditation, expansion of scope, and the testing laboratory approval process can be found in Annex C.

The NIAP Validation Body assesses the results of a security evaluation conducted by a CCTL within the scheme and when appropriate, issues a *Common Criteria certificate*. The certificate, together with its associated validation report, confirms that an IT product or protection profile has been evaluated at an accredited testing laboratory using the Common Methodology for conformance to the Common Criteria. The certificate also confirms that the IT security evaluation has been conducted in accordance with the provisions of the scheme and that the conclusions of the testing laboratory are consistent with the evidence presented during the evaluation.

The Validation Body maintains a *NIAP Validated Products List* containing all IT products and protection profiles successfully completing evaluation and validation under the scheme. The validated products list also includes those products and profiles successfully completing similar processes under the schemes of authorized signatories to the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security*.<sup>9</sup>

In order for IT products to receive Common Criteria certificates and be placed on the NIAP Validated Products List, evaluations must be performed against explicit security targets. A security target may or may not claim conformance to a protection profile. A security target claiming conformance to a particular protection profile must be evaluated against that profile to substantiate the claim. This evaluation is conducted in addition to, and in conjunction with, the evaluation of the actual IT product against its security target.

The cost of an IT security evaluation will be determined strictly by the individual contract negotiations between the sponsor of the evaluation and testing laboratory selected to conduct the evaluation. The NIAP Validation Body does not play any role in sponsor-laboratory contract negotiations. The Validation Body will, however, provide validation services for sponsors and CCTLs at no charge during the initial two-year period of scheme operation. The actual cost of these services to include technical oversight and monitoring, final issuance of Common Criteria certificates, publication of validation reports, and the posting of IT products and protection profiles

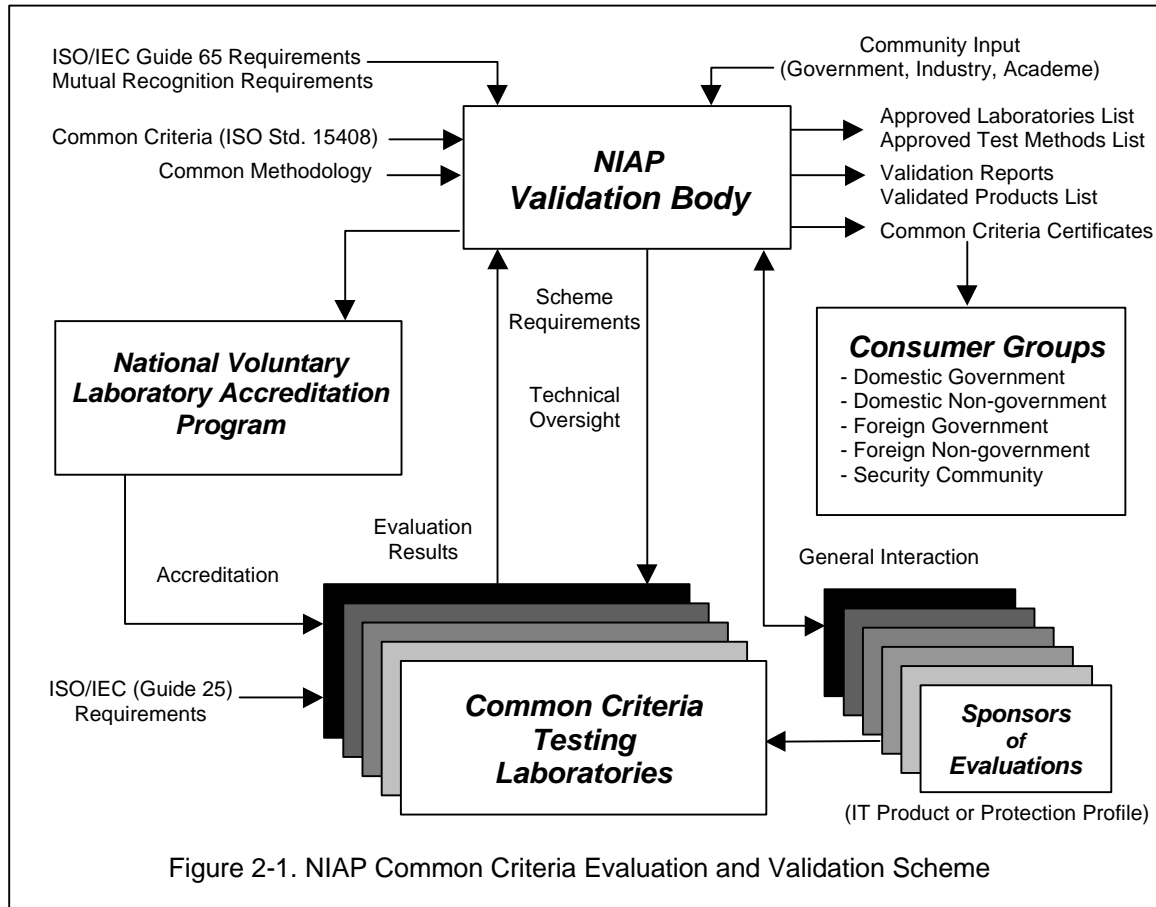
---

<sup>8</sup> In the scheme, a test method is defined to be a Common Criteria assurance package and the associated evaluation methodology for that assurance package from the Common Methodology. Initially, the scheme will provide a limited number of test methods, primarily corresponding to the Common Criteria Evaluation Assurance Levels (EALs) 1 through 4 and the associated evaluation methodology for those EALs. Test methods for protection profile and security target evaluations will also be offered. Additional test methods may be subsequently defined based on consumer requirements, technical viability, and scheme experience.

<sup>9</sup> The *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security* is a multilateral agreement among Parties that share common objectives with respect to IT products and protection profiles. These objectives are: to ensure that evaluations are performed to high and consistent standards; to improve the availability of evaluated products and profiles for national use; to eliminate duplicate evaluations; and to continuously improve the efficiency and cost-effectiveness of the evaluation and validation processes. The purpose of the Agreement is to advance those objectives by bringing about a situation in which IT products and protection profiles which earn a Common Criteria certificate can be procured or used without the need for them to be evaluated and validated again.

on the NIAP Validated Products List will be monitored and assessed during that initial period. The Validation Body intends to initiate a cost-recovery program for validation services after the initial two-year period.

Figure 2-1 illustrates the relationships among key participants within the Common Criteria Scheme.



### **3 Roles and Responsibilities**

This chapter describes the roles and responsibilities of the principal participants in the Common Criteria Scheme, (i.e., sponsors of IT security evaluations, the NIAP Validation Body, and Common Criteria Testing Laboratories). Additional details regarding the roles and responsibilities of participants can be found in the supporting Annexes to this document.

#### **3.1 Sponsor of an IT Security Evaluation**

The *sponsor* is the individual or organization requesting a security evaluation of an IT product or a protection profile. The relationship of the sponsor to the IT product or protection profile may vary depending on the nature of the product or profile and the circumstances surrounding the evaluation. In most cases, the sponsor of a security evaluation will be the actual developer of the IT product or protection profile. However, this may not always be the case. The sponsor of a security evaluation may be a value-added reseller of an IT product or an organization or individual involved in the acquisition of an IT system that includes that particular product as a key component. The sponsor may also be an independent contractor, serving as a systems developer or integrator attempting to fulfill the requirements of a contract. Consortia or trade associations may nominate a single point of contact to serve as the sponsor of an evaluation.

In cases where the sponsor of an evaluation is not the developer of the product or protection profile, the sponsor needs to obtain the cooperation of the developer in providing the CCTL with technical materials and essential deliverables necessary to conduct the IT security evaluation in a complete and consistent manner. The specific details of the provision of documentation for the security evaluation will be handled in contractual agreements between the sponsor and the IT product or protection profile developer. The specific obligations of the sponsor of an evaluation are outlined in Annex D. Additional sponsor-related information can be found in Scheme Publication #5 *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Guidance to Sponsors of Evaluations*.

#### **3.2 NIAP Validation Body**

The principal objective of the NIAP Validation Body is to ensure the provision of competent IT security evaluation and validation services for both government and industry. The Validation Body has the ultimate responsibility for the operation of the scheme in accordance with its policies and procedures, and where appropriate, for the interpretation and amendment of those policies and procedures. NIST and NSA are responsible for providing sufficient resources to the Validation Body so that it may carry out its responsibilities.

The NIAP Validation Body must ensure that appropriate mechanisms are in place to protect the interests of all parties within the scheme participating in the process of IT security evaluation. Any dispute brought forth by a participating party, (i.e., sponsor of an evaluation, product or protection profile developer, or CCTL), concerning the operation of the scheme or any of its associated activities shall be referred to the Validation Body for resolution. In disputes involving the Validation Body, NIST and NSA management will attempt to resolve the dispute through procedures agreed upon by the two organizations.

The Validation Body is led by a Director and Deputy Director selected by NIST and NSA management. The Director and Deputy Director cannot be filled from the same agency. The Director of the Validation Body reports to the NIAP Director for administrative and budgetary matters and to the NIST and NSA certificate-issuing authorities for scheme-related operational matters. In general, the Director and Deputy Director serve a two-year term of service. This term of service may be extended at the discretion of NIST and NSA management. There are also a

significant number of technical and administrative support personnel required to provide a full range of validation services for the sponsors of evaluations and the CCTLs. These personnel include validators, technical experts in various technology cells, and senior members of the technical staff and the IT security community on the Oversight Board. In particular, the Validation Body staff is organized as follows:

- a) Director (NIST or NSA);
- b) Deputy Director (NIST or NSA);
- c) Technical Advisor: (NIST or NSA);
- d) Oversight Board: (NIST, NSA, NVLAP, Industry);
- e) Technical staff members (NIST and NSA);
- f) Administrative staff members (NIST and NSA);
- g) Contractual support (as needed).

In general, the responsibilities of the Validation Body are:

- a) to establish policy and procedures for the operation of the scheme, and to ensure that the policies and procedures of the scheme are followed;
- b) to document the organization, policy, and procedures of the scheme and to make that information available to the public;
- c) to approve CCTL participation in the scheme;
- d) to monitor the performance of participating CCTLs and in particular, their adherence to, and application and interpretation of, the Common Criteria and the Common Methodology;
- e) to remove a CCTL from the NIAP Approved Laboratories List if the laboratory fails to meet the terms and conditions of the scheme;
- f) to provide notice to the community of any changes to the NIAP Approved Laboratories List including additions or withdrawals of CCTLs from the scheme and any modifications to the scope of a laboratory's accreditation;
- g) to ensure that appropriate procedures are in place within the scheme to protect sensitive or proprietary information relating to IT products or protection profiles under evaluation and that those procedures are routinely followed;
- h) to provide advice, guidance, support, and standards for training to CCTLs as required;
- i) to review evaluation technical reports from CCTLs to ensure that the conclusions are consistent with the evidence presented and that the Common Criteria and the Common Methodology have been correctly applied;
- j) to ensure consistency of CCTL evaluations across the scheme through the activities of its Oversight Board;
- k) to seek guidance from industry experts, (e.g., consumer groups, IT product or protection profile developers, testing laboratories, researchers, standards groups), when resolving

disputes, addressing challenges, answering technical questions or taking critical decisions regarding any aspect of the scheme;

- l) to publish publicly-releasable *validation reports* and issue Common Criteria certificates for each successful evaluation submitted;
- m) to publish at regular intervals, a validated products list, giving the particulars of all IT products and protection profiles evaluated for which validation reports have been published and Common Criteria certificates issued;
- n) to include in its validated products list, IT products and protection profiles completing evaluation and validation under the authority of other nations and receiving certificates in accordance with the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security*;
- o) to ensure that all necessary logos and marks are appropriately placed on Common Criteria certificates or any other documents requiring such identification;
- p) to ensure that the interests of all parties participating in scheme activities are given appropriate consideration;
- q) to arbitrate disputes arising in the context of the scheme;
- r) to approve press releases or similar statements relating to the scheme;
- s) to publish an annual report describing the scheme activities.

Specific requirements for the Validation Body are outlined in Annex B.

In order to carry out its scheme responsibilities and fulfill the conditions of the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security*, the Validation Body must maintain a high degree of technical expertise and competence in all aspects of security testing and evaluation. This expertise is critical to conducting validations and providing the necessary technical support to sponsors of evaluations and to CCTLs participating in the scheme. To that end, the Validation Body reserves the right to place its technical personnel in selected CCTLs for the express purpose of observing and/or participating in Common Criteria-based evaluations in a variety of technology areas. This training activity will be called *shadow evaluation*.

The Validation Body will coordinate closely with the management and staff of CCTLs participating in shadow evaluations to ensure that the activities do not adversely impact any ongoing evaluations being conducted by the testing laboratories. The Validation Body shall incur no costs from shadow evaluations other than the cost of funding NIAP technical personnel assigned to CCTLs. Additional details regarding shadow evaluations and other training-related activities are provided in Scheme Publication #2, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Validation Body Standard Operating Procedures*.

### **3.3 Common Criteria Testing Laboratories**

CCTLs are testing laboratories that are accredited by NVLAP and listed on an approved laboratories list by the NIAP Validation Body. These laboratories must meet the requirements of:

- a) NIST Handbook 150, *Procedures and General Requirements*,<sup>10</sup>
- b) NIST Handbook 150-20, *Information Technology Security Testing—Common Criteria*;
- c) Specific criteria for IT security evaluations and other requirements of the scheme as defined by the NIAP Validation Body (see Annex C).

CCTLs enter into contractual agreements with sponsors to conduct security evaluations<sup>11</sup> of IT products and protection profiles using NIAP-approved test methods derived from the Common Criteria, Common Methodology and other technology-based sources. The IT security evaluations are carried out in accordance with the policies and procedures of the scheme.

CCTLs must observe the highest standards of impartiality, integrity, and commercial confidentiality, and operate within the guidelines established by the scheme. With respect to commercial confidentiality, CCTLs must have documented policy and procedures to ensure the protection of sensitive or proprietary information. These procedures shall be subject to audit by NVLAP and the NIAP Validation Body.

Neither the CCTL, nor any individual CCTL staff members concerned with a particular IT security evaluation, may have a vested interest in the outcome of that evaluation. A CCTL staff member or evaluation team cannot, under any circumstances, be involved in:

- a) both the development and evaluation of the same IT product or protection profile;
- b) the provision of consultancy services to the sponsor of an evaluation or a product/profile developer which would compromise the independence of the evaluation.

Accordingly, CCTLs must ensure that any activities related to the production of evaluation evidence for a particular IT product or protection profile preparing to enter evaluation (within that same testing laboratory) do not conflict with the laboratory's ability to conduct a fair and impartial evaluation of that product or profile. The above conflict of interest guidelines will be subject to the scrutiny of the NIAP Validation Body and NVLAP to ensure these conditions are met. The Validation Body and NVLAP will be the final arbiters in determining potential or actual conflicts of interest which may threaten the integrity of security evaluations conducted within the scheme.

A CCTL shall provide the Validation Body with thirty days notice of its intention to withdraw from the scheme. Additional laboratory-related information can be found in Scheme Publication #4 *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Guidance to Common Criteria Testing Laboratories*.

### **3.4 Guidance for Consumers**

It is important that consumers of IT products and protection profiles understand how to interpret the results of IT security evaluations conducted within the scheme. These results are described in *evaluation technical reports* produced by the CCTLs and summarized in the associated validation reports and Common Criteria certificates published by the NIAP Validation Body.

<sup>10</sup> NIST Handbook 150 contains the requirements of ISO/IEC Guide 25, *General Requirements for the Competence of Calibration and Testing Laboratories*. ISO/IEC Technical Report 13233, *Information Technology-Interpretation of Accreditation Requirements in Guide 25 Accreditation of Information Technology and Telecommunications Testing Laboratories for Software and Protocol Testing Services* is used by NVLAP to interpret the requirements of ISO/IEC Guide 25 for CCTLs.

<sup>11</sup> The purpose of a security evaluation is to confirm that an IT product meets its security target. To accomplish this, CCTL evaluators must understand the product, its security policy, and how the security features enforce the product's security policy. Evaluators must also test the security features of the product and write a final evaluation technical report describing their analysis and testing.

An IT product is typically evaluated in a generic laboratory setting at a CCTL within the scheme. In that regard, there are some general assumptions made about the operational environment where the product is ultimately to be employed subsequent to the security evaluation. In some cases, an evaluated IT product may be integrated into a more complex configuration of products that compose an IT system. The actual environment of use may also be significantly different from the one described in the original assumptions set forth in the security target. In the end, consumers must assess the overall contribution to assurance made by the evaluated IT product. When making that assessment, there are several things a consumer should consider:

- a) The accuracy and completeness of security evaluation results are dependent on the accuracy and completeness of the information and documentation provided to the CCTL by the sponsor of the evaluation;
- b) The quality of a security target, (i.e., security specification), and the reported results of an IT product evaluated against that security target, are a function of how well the product is able to be described under the Common Criteria and the degree to which the Common Methodology and the derivative test methods are able to measure conformance to the security target;
- c) The security evaluation results are only applicable to that particular version and release of the product in its evaluated configuration. Consumers are responsible for determining the security impact of installing or operating an evaluated IT product in a configuration other than the configuration in which it was evaluated.

## 4 IT Security Evaluation

This chapter describes the activities of the Common Criteria Scheme participants during the various stages of an IT security evaluation.<sup>12</sup>

### 4.1 Preparation for IT Security Evaluation

The majority of activity in the early stages of an evaluation takes place between the sponsor of the evaluation and CCTL. The sponsor is responsible for providing the security target and the associated IT product that will become the Target of Evaluation (TOE). The composition of a TOE may be varied and consist of hardware, firmware, and software (or any combination thereof). The TOE may also include multiple IT products (sometimes referred to as an IT system), some of which may already be evaluated. All security-relevant information and documentation produced during the IT product development process shall be included in the deliverables supplied to the CCTL conducting the evaluation. The sponsor must ensure that arrangements have been made to provide all essential documentation to the CCTL in order to conduct a successful security evaluation.

#### 4.1.1 Consultancy Work in Support of Evaluations

The scope of consultancy work during the preparation for an IT security evaluation is not controlled by the scheme and is a matter for negotiation between the sponsor and the CCTL or other consultant. However, the CCTL must adhere to the terms and conditions of its NVLAP accreditation to ensure that the advice given does not affect evaluator independence or impartiality in any evaluation.

For each evaluation, CCTLs shall notify the Validation Body of any consultancy activities conducted on behalf of a sponsor of an evaluation that are relevant to that evaluation. These activities must not inhibit the CCTL from demonstrating that its independence and impartiality will be maintained during the evaluation.

#### 4.1.2 Security Target

The security target serves as both a specification of the security functions against which the IT product, (i.e., TOE), will be evaluated and as a description relating the product to the environment in which it will operate. The sponsor of an evaluation provides the security target, which includes a list of claims about the IT product made by the sponsor. The content and presentation of the security target must be specified in terms of the Common Criteria. The security target may also claim conformance to a protection profile.

#### 4.1.3 Deliverables

The deliverables for an IT security evaluation are typically items of hardware, firmware, software or other technical documentation normally generated during the development of the product. The sponsor of an evaluation must ensure the timely supply of deliverables for the evaluation. Appropriate contractual arrangements shall be made by the sponsor to ensure the supply of evaluation deliverables to the CCTL. If the TOE consists of multiple IT products, some of which have been previously evaluated, the sponsor of the evaluation must ensure that contractual arrangements include authority for the release of previous evaluation results.

---

<sup>12</sup> This chapter focuses primarily on the evaluation of IT products. Therefore, some of the information is not applicable to the evaluation of protection profiles. Section 4.4 provides additional information regarding protection profile evaluations.



The sponsor of an IT security evaluation must ensure that the CCTL and the Validation Body have access to any proprietary information necessary to conduct the evaluation and validation, respectively. The CCTL may be unable to perform an evaluation of the product and the Validation Body may be unable to publish its validation report if access to such proprietary information is denied.

The Validation Body and CCTL shall ensure that no sensitive or proprietary information is released to unauthorized parties during the course of an evaluation that would in any way compromise this information. The CCTL shall ensure that the nature and extent of the proprietary information is defined and apply appropriate rules for its protection.

#### 4.1.4 Readiness for Evaluation

Once the sponsor has established the security target and the strategy for the supply of deliverables, the sponsor should approach a CCTL to initiate the evaluation of the product. A sponsor may also use the completed security target to obtain evaluation proposals from CCTLs.

The CCTL selected to conduct the evaluation should review the security target to ensure that it provides a sound basis for the evaluation.<sup>13</sup> The sponsor should be notified of any problems so that the security target can be amended prior to the start of the evaluation. When a successful evaluation seems to be feasible, the selected CCTL should prepare a TOE-specific *evaluation work plan*, an *evaluation schedule*, and a *deliverables list*.

#### 4.1.5 Entering the Scheme

The NIAP Validation Body becomes involved in an IT security evaluation when the sponsor and the CCTL selected to conduct the evaluation notify the Validation Body of the proposed evaluation and request formal acceptance of the evaluation into the scheme. The Validation Body needs certain items of information from the sponsor and the CCTL before accepting the prospective evaluation into the scheme. These items include:

- a) the security target and description of the TOE;
- b) evaluation work plan;
- c) evaluation schedule.

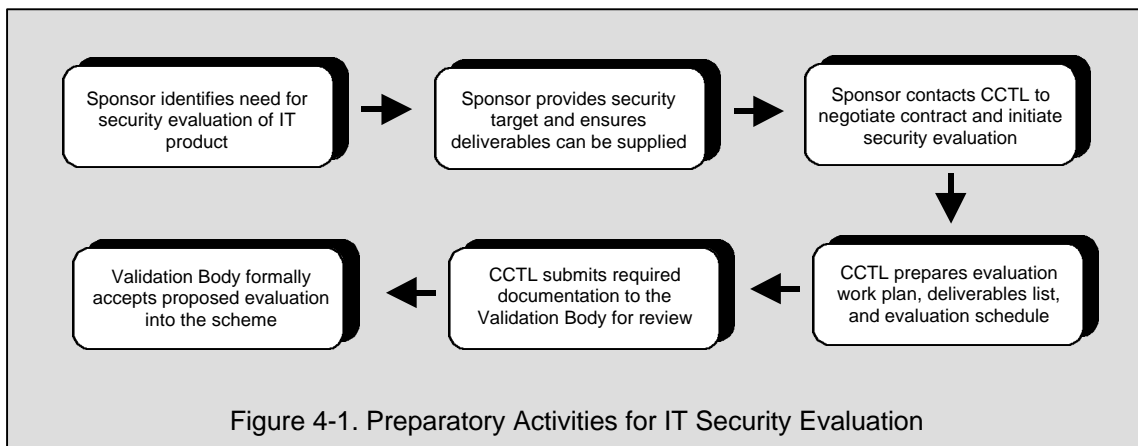
As part of its formal acceptance of the evaluation into the scheme, the Validation Body reviews the documentation presented by the sponsor and the CCTL to assess whether all parties have done adequate preparation for the proposed evaluation. This initial review may include meetings with the sponsor and key personnel from the CCTL and is intended to mitigate risk on behalf of all participants in the evaluation and validation processes. The specific activities associated with this review process are described in Scheme Publication #3, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Technical Oversight and Validation Procedures*.

In order to adequately support the technical oversight and validation activities required by the NIAP Validation Body in fulfillment of its obligations under the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security*, CCTLs are strongly cautioned not to begin actual evaluation tasks until the proposed evaluation is formally accepted into the scheme.

---

<sup>13</sup> This informal review of the security target by the CCTL should not be confused with the formal evaluation of the security target conducted by the laboratory in accordance with the requirements of the Common Criteria and Common Methodology.

Figure 4-1 summarizes the activities associated with preparation for evaluation.



## 4.2 Conduct of the IT Security Evaluation

Evaluation is the assessment of an IT product for conformance to the Common Criteria. The evaluation determines how well the product, or TOE, upholds its functional and assurance security specification contained in its security target. The objective is to enable the CCTL conducting the evaluation to prepare an impartial report stating whether or not the TOE satisfies its security target.<sup>14</sup>

The CCTL conducts the IT security evaluation of the TOE according to the evaluation work plan using the deliverables specified in the deliverables list. The work plan may evolve during the evaluation as additional information is made available to the CCTL by the sponsor. The CCTL is encouraged to consult with the Validation Body at any time to discuss technical matters, anomalies which may arise, or any other issues relevant to the evaluation.

The results of the IT security evaluation are documented by the CCTL as the evaluation proceeds. The sponsor and CCTL shall inform the Validation Body through *observation reports*<sup>15</sup> of issues that arise during evaluation to include problems found in the TOE and any problems related to the Common Criteria or Common Methodology. In general, CCTLs should be interacting directly with sponsors to resolve issues and address problems that arise during an evaluation. Observation reports should be submitted only in situations where:

- a) specific issues or problems could not be resolved by the sponsor and CCTL;
- b) guidance or interpretation from the Validation Body is required.

In situations where the issue or problem is product-related, the sponsor shall provide the Validation Body and the CCTL a detailed proposal for the resolution of the issue or problem noted

<sup>14</sup> The first phase of a formal security evaluation is the evaluation of the security target itself in accordance with the requirements described in the Common Criteria and Common Methodology. Following security target evaluation, the IT product, or TOE, is evaluated against the security target. These activities are occasionally interleaved during an evaluation.

<sup>15</sup> An observation report is a vehicle by which a CCTL or sponsor of an evaluation requests a clarification of scheme-related information or identifies an anomaly in the evaluation. Observation reports can also be submitted by members of the Validation Body. Typically, the report will contain the observation, severity of the observation, organization responsible for resolving the issue, timetable for resolution of the issue, and impact on the evaluation if the issue is not resolved.

in the report and the timeframe for such activity. If it is not possible to resolve a particular issue or problem, and the Validation Body decides that the evaluation will be affected, the Validation Body shall contact the sponsor to discuss the potential impact and possible alternatives. Based on the contract with the CCTL, the sponsor may:

- a) abandon the IT security evaluation;
- b) consult with the Validation Body to discuss continuing the security evaluation while accepting the problem and its implication for validation;
- c) reschedule the security evaluation and, in consultation with the Validation Body, ensure that the TOE is modified, as needed.

In situations where the issue or problem is related to the Common Criteria, the Common Methodology, or the scheme, the Validation Body will take the following actions, in turn, upon receipt of the observation report:

- a) assess the immediate issue or problem and render an initial decision for that particular IT security evaluation;<sup>16</sup>
- b) address the issue or problem within scheme channels, employing the services of technical working groups with security and testing community representation from CCTLs and other technical experts as needed;
- c) if necessary, address the problem or issue formally within international channels in accordance with established procedures and involving relevant standards groups, technical committees, or other appropriate bodies.

### **4.3 Conclusion of the Evaluation**

The findings of the IT security evaluation are documented by the CCTL in an evaluation technical report. The content and presentation of evidence in the report shall be in accordance with the Common Criteria and Common Methodology. The CCTL shall ensure that the evaluation technical report is structured in such a way as to allow for the removal of proprietary or sensitive information.

Two versions of the report are submitted to the Validation Body and to the sponsor of the evaluation:<sup>17</sup>

- a) a complete evaluation technical report (including proprietary and/or sensitive information);
- b) an abridged, evaluation technical report (complete report excluding only proprietary and/or sensitive information).

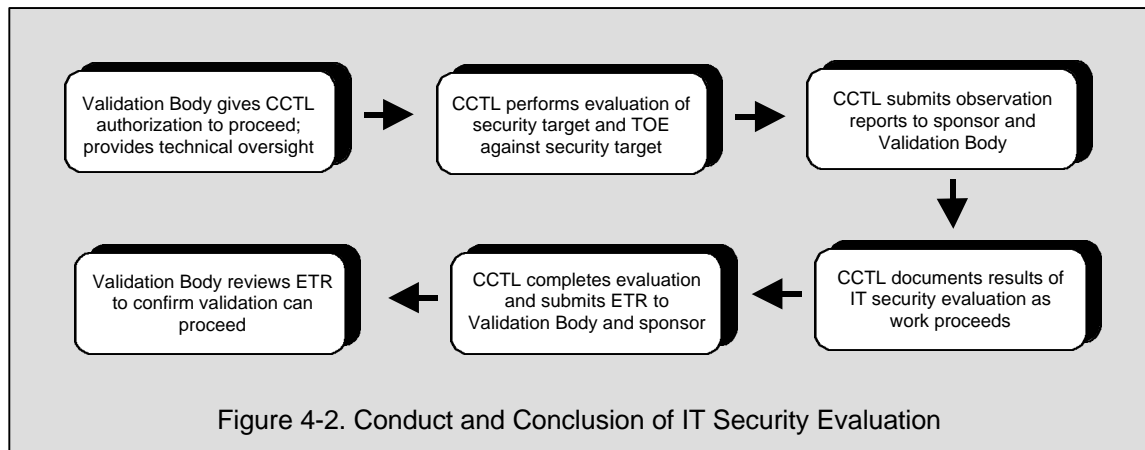
The sponsor may contact the CCTL concerning any statements in the report which the sponsor believes to be misleading, unjustified, or inaccurate.

---

<sup>16</sup> The purpose of this immediate decision is to expedite the IT security evaluation and not adversely impact the CCTL's evaluation schedule. The decision applies only to the current evaluation in question (on a temporary, one-time basis) and is to be subsequently considered in a more formal setting by the appropriate technical committees or working groups either within the scheme or through counterpart organizations within the international community.

<sup>17</sup> It is assumed that in situations where the sponsor of an evaluation is not the product developer, appropriate arrangements will be made regarding the release of proprietary and/or sensitive information to the sponsor.

Figure 4-2 summarizes the activities associated with the conduct and conclusion of the IT security evaluation.



#### 4.4 Evaluation of Protection Profiles

The goal of protection profile evaluation is to demonstrate that the profile is complete, consistent, and technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated. The sponsor is responsible for providing the protection profile to the CCTL conducting the evaluation. In addition, the sponsor may want to provide the CCTL any relevant documentation associated with the development of the protection profile.

The Validation Body needs certain items of information from the sponsor and the CCTL before accepting the prospective protection profile evaluation into the scheme. These items include:

- a) the protection profile;
- b) evaluation work plan;
- c) evaluation schedule.

As with IT product evaluations, the findings of the protection profile evaluation are documented by the CCTL in an evaluation technical report. The content and presentation of evidence in the report shall be in accordance with the appropriate sections of the Common Criteria and the Common Methodology. The report is submitted to the Validation Body and to the sponsor of the evaluation. The sponsor may contact the CCTL concerning any statement in the protection profile evaluation technical report which the sponsor believes to be misleading, unjustified, or inaccurate.



## 5 Technical Oversight and Validation

This chapter describes the activities associated with the technical oversight of IT security evaluations, the validation process, issuance of Common Criteria certificates, and the publication of the NIAP Validated Products List. It also introduces the concept of certificate maintenance.

### 5.1 Technical Oversight

Technical oversight is the general process employed by the NIAP Validation Body to ensure that the evaluation and validation activities taking place within the scheme are being conducted in accordance with the provisions of the Common Criteria, the Common Methodology, the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security*, and any scheme-specific policies and procedures. Technical oversight involves the monitoring of CCTLs and the monitoring of specific evaluations.

The Common Criteria Scheme focuses on the laboratory accreditation process to ensure that commercial testing facilities have the requisite capability to conduct quality security evaluations of IT products and protection profiles in a consistent manner. However, the complexity of IT security evaluations with the dual requirements for design analysis and testing makes these types of evaluations unique. This complexity and need for consistency across the scheme to ensure fairness for all participating CCTLs, make technical oversight essential.

Technical oversight begins with the acceptance of an IT security evaluation into the scheme by the NIAP Validation Body. During the evaluation, the Validation Body routinely interacts with the CCTL and the sponsor of the evaluation by:

- a) providing information in technical and non-technical areas deemed essential to the success of the IT security evaluation;<sup>18</sup>
- b) requiring and receiving information in technical and non-technical areas deemed essential to the validation process;
- c) working together to resolve important technical issues.

Technical oversight will be exercised by the Validation Body as required to adequately ensure that the CCTL has correctly and completely applied the Common Criteria and the Common Methodology for the specific IT security evaluation and level of assurance sought. The purpose of technical oversight and evaluation monitoring is to mitigate risk among all participants in the scheme, (i.e., the NIAP Validation Body, CCTLs, and sponsors of evaluations). In general, the number, type, and intensity of activities associated with the oversight process will be a function of:

- a) the assurance requirements, (i.e., predefined Common Criteria evaluation assurance level or sponsor-defined assurance package), that appear in the security target;
- b) the complexity of the Target of Evaluation (TOE);
- c) the experience of the CCTL in evaluating IT products in the identified technology area.

---

<sup>18</sup> The Validation Body provides information to sponsors and CCTLs in a variety of areas supporting IT product and protection profile evaluations. This support includes, but is not limited to, guidance for evaluating specific information technologies, tutorial information on the Common Criteria and Common Methodology, interpretations of criteria, and application of methodology.

The Validation Body will issue strict guidelines on how these technical oversight activities will be implemented within the scheme in order to establish the appropriate level of expectation on behalf of sponsors and CCTLs. The specific details of the technical oversight process and activities associated with that process are described in Scheme Publication #3, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Technical Oversight and Validation Procedures*.

## **5.2 The Validation Process**

Validation provides independent confirmation that an IT security evaluation has been conducted in accordance with the provisions of the scheme and that the conclusions of the CCTL are consistent with the facts presented in their evaluation technical report. The Validation Body uses the validation process to ensure that consistent technical decisions are taken in applying the Common Criteria and Common Methodology across evaluations within the scheme. The validation process culminates in the publication of a formal report and the issuance of a Common Criteria certificate by the Validation Body.

The Validation Body shall assign a technical representative, or *validator*, to each IT security evaluation to serve as the primary point of contact for the CCTL and sponsor of the evaluation. The CCTL and sponsor shall also assign a point of contact to interact with the Validation Body during the evaluation. The Validation Body shall have its technical representative monitor the evaluation and perform a variety of validation activities as described in Scheme Publication #3, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Technical Oversight and Validation Procedures*. Depending on the specific validation requirements for a particular evaluation, validators may attend evaluation progress reviews or other meetings with the CCTL and/or sponsor, as deemed necessary for the success of the evaluation and validation.

Upon completion of the security evaluation, the Validation Body reviews the evaluation technical report produced by the CCTL. This review determines the extent to which the security target is met by the TOE. In the case of a protection profile evaluation, the review determines the extent to which the profile is shown to be complete, consistent, and technically sound. The Validation Body also confirms that the evaluation was conducted in accordance with the Common Criteria, Common Methodology, and procedures required by the scheme and that the report provides a suitable basis for the final validation report.

The Validation Body reserves the right to contact the CCTL to obtain additional information for clarification of evaluation-related issues and/or obtain access to specific evidence and results to support any conclusions presented in the evaluation technical report. The specific activities involved in the review process are described in Scheme Publication #3, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Technical Oversight and Validation Procedures*.

The findings of the IT security evaluation shall be documented in the final validation report, prepared by the validator in consultation with selected technical representatives from the NIAP Validation Body. The validation report is composed largely of information derived from the evaluation technical report produced by the CCTL. The purpose of the report is to provide a statement of how well the TOE conforms to its security target, or how well the protection profile meets the requirements in the Common Criteria and Common Methodology. The issue of a validation report by the NIAP Validation Body does not imply that the TOE is guaranteed to be completely free of exploitable vulnerabilities or that the protection profile provides a suitable set of security requirements for particular operational environments.

After review within the Validation Body, the draft validation report is issued to the sponsor of the evaluation and the CCTL for confirmation of the following:

- a) the conclusions of the report are accurate;
- b) there are not any factors which could invalidate the report;
- c) all proprietary and/or sensitive information has been purged.

Subsequent to the external review by the sponsor and CCTL, the final evaluation technical report is presented by the validator to the NIAP Validation Body's Oversight Board for review and comment. Upon approval by the Oversight Board, the Validation Body publishes the final validation report which summarizes and confirms the results of an evaluation conducted by a CCTL, (i.e., the evaluation has been properly carried out and that the Common Criteria, Common Methodology, and other procedures have been correctly applied, and that the conclusions of the CCTL are consistent with the evidence adduced). The validation report will be a public document, free from proprietary or sensitive information, and remain the property of the Validation Body. Reproduction and distribution of the validation report by the sponsor is authorized by the Validation Body provided the report is copied in its entirety.

### **5.3 Common Criteria Certificates**

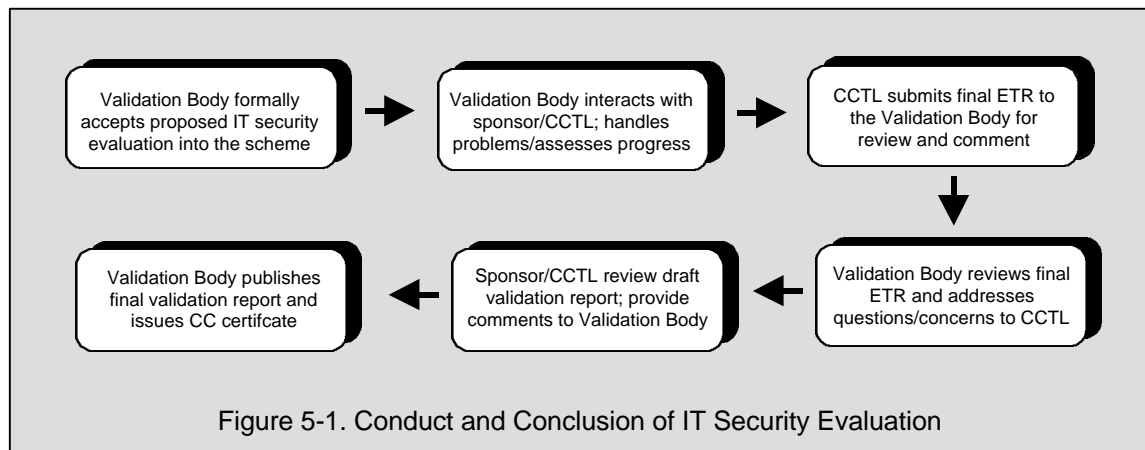
Once the final validation report has been approved by the Validation Body, a Common Criteria certificate will be issued. NIST and NSA, as joint partners in NIAP, are the certificate-issuing authorities for the scheme. A senior executive from each agency will sign the certificate, indicating acceptance of the points articulated above. After the certificate has been issued to the sponsor of the security evaluation, an appropriate entry will be made on the NIAP Validated Products List.

The certificate applies only to the specific version and release of the IT product in its evaluated configuration or the particular version of the protection profile as evaluated. A sponsor of an evaluation shall only market an IT product or a protection profile as an evaluated product or an evaluated profile, respectively, on the basis of the validation report and accompanying Common Criteria certificate published by the Validation Body. The issuance of a certificate does not imply endorsement of an IT product or protection profile by NIST, NSA, or any other agency of the U.S. Government. Additional details on Common Criteria certificates can be found in Annex E.

Procedures for the maintenance of Common Criteria certificates, (e.g., in conjunction with extensions to later releases or versions of the IT product or protection profile), are governed by the Common Criteria Certificate Maintenance Program as described in Annex F. A sponsor, anticipating the need for re-evaluation, may wish to consider a certificate maintenance approach at early stages of the initial evaluation in order to minimize future evaluation activities. Sponsor coordination with a CCTL may be required in order to take re-evaluation or certificate maintenance requirements into account when performing the initial evaluation of the IT product or protection profile. Specific details of the certificate maintenance process employed within the scheme are provided in Annex F.



Figure 5-1 summarizes the activities associated with technical oversight and the validation process.



## References

- [CIP97] The Report of the President's Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations: Protecting America's Infrastructures*, October, 1997.
- [CIP98] The White House, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 1998.
- [CEM98] CEMEB (Common Evaluation Methodology Editorial Board), *Common Methodology for Information Technology Security Evaluation*, Version 1.0, August 1999 (projected).
- [COM98] CCEB (Common Criteria Editorial Board), *Common Criteria for Information Technology Security Evaluation*, Version 2.0, May 1998.
- [DOD85] DOD (U.S. Department of Defense), *Trusted Computer System Evaluation Criteria*, DOD5200.28-STD, December 1985.
- [FED92] NIST (National Institute of Standards and Technology) and NSA (National Security Agency), *Federal Criteria for Information Technology Security*, Version 1.0, December 1992.
- [ISO90] ISO/IEC Guide 25—*General Requirements for the Competence of Calibration and Testing Laboratories*, 1990.
- [ISO96] ISO/IEC Guide 65—*General Requirements for Bodies Operating Product Certification Systems*, 1996.



## Acronym List

AMP	Assurance Maintenance Plan
CC	Common Criteria (for IT Security Evaluation)
CM	Common Methodology (for IT Security Evaluation)
CMP	Certificate Maintenance Program
CMR	Certificate Maintenance Report
CMSR	Certificate Maintenance Summary Report
CCTL	Common Criteria Testing Laboratory
CCEVS	Common Criteria Evaluation and Validation Scheme
ETR	Evaluation Technical Report
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
LAP	Laboratory Accreditation Program
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PP	Protection Profile
ST	Security Target
TTAP	Trust Technology Assessment Program
TOE	Target of Evaluation
VB	Validation Body
VR	Validation Report
VPL	Validated Products List

## Publications List

Scheme Publication #1 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Organization, Management, and Concept of Operations*

Scheme Publication #2 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Validation Body Standard Operating Procedures*

Scheme Publication #3 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Technical Oversight and Validation Procedures*

Scheme Publication #4 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Guidance to Common Criteria Testing Laboratories*

Scheme Publication #5 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Guidance to Sponsors of IT Security Evaluations*

Scheme Publication #6 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Certificate Maintenance Program*

NIST Handbook 150 *Procedures and General Requirements*

NIST Handbook 150-20 *Information Technology Security Testing—Common Criteria*

**\*\* Refer to NIAP web site for current information on publication dates and version numbers.**

## Annex A. Glossary

This glossary contains definitions of terms used in the Common Criteria Scheme. These definitions are consistent with the definitions of terms in ISO Guide 2 and also broadly consistent with the Common Criteria and Common Methodology. However, the definitions of terms may have been amplified to add greater clarity or to interpret in the context of the evaluations conducted within the scheme.

**Accredited:** Formally confirmed by an accreditation body as meeting a predetermined standard of impartiality and general technical, methodological, and procedural competence.

**Accreditation Body:** An independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the standard.

**Agreement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security:** An agreement in which the Parties (i.e., signatories from participating nations) agree to commit themselves, with respect to IT products and protection profiles, to recognize the Common Criteria certificates which have been issued by any one of them in accordance with the terms of the agreement.

**Approval Policy:** A part of the essential documentation of the Common Criteria Evaluation and Validation Scheme, setting out the procedures for making an application to be approved as a CCTL and placed on the NIAP Approved Laboratories List and for the processing of such applications and of the requirements which an applicant must fulfill in order to qualify.

**Approved:** Assessed by the NIAP Validation Body as technically competent in the specific field of IT security evaluation and formally authorized to carry out evaluations within the context of the Common Criteria Evaluation and Validation Scheme.

**Approved Laboratories List:** The list of approved CCTLs authorized by the NIAP Validation Body to conduct IT security evaluations within the Common Criteria Evaluation and Validation Scheme.

**Approved Test Methods List:** The list of approved test methods maintained by the NIAP Validation Body which can be selected by a CCTL in choosing its scope of accreditation, that is, the types of IT security evaluations that it will be authorized to conduct using NIAP-approved test methods.

**Assurance Maintenance Plan:** Part of the formal assurance maintenance documentation submitted to the Validation Body by the sponsor of an evaluation (as part of the initial TOE evaluation) that identifies the plans and procedures a developer is to implement in order to ensure that the assurance that was established in the validated TOE is maintained as changes are made to the TOE or its environment.

**Availability:** The prevention of unauthorized withholding of information resources.

**Certificate Maintenance Program:** A program within the Common Criteria Scheme that allows a sponsor to maintain a Common Criteria certificate by providing a means (through specific assurance maintenance requirements) to ensure that a validated TOE will continue to meet its security target as changes are made to the IT product or its environment.

**Certificate Maintenance Report:** A report prepared by a CCTL for the Validation Body detailing the results of their evaluation maintenance activities conducted on behalf of a sponsor.

**Certificate Maintenance Summary Report:** An annual report prepared by a sponsor for the Validation Body providing a summary of all certificate maintenance activities conducted during the previous year.

**Common Criteria (CC):** Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.

**Common Methodology (CM):** Common Methodology for Information Technology Security Evaluation, the title of a technical document which describes a particular set of IT security evaluation methods.

**Common Criteria Certificate:** A brief public document issued by the NIAP Validation Body under the authority of NIST and NSA which confirms that an IT product or protection profile has successfully completed evaluation by a CCTL. A Common Criteria certificate always has associated with it, a validation report.

**Common Criteria Evaluation and Validation Scheme:** The program developed by NIST and NSA as part of the National Information Assurance Partnership (NIAP) establishing an organizational and technical framework to evaluate the trustworthiness of IT products and protection profiles.

**Common Criteria Testing Laboratory (CCTL):** Within the context of the Common Criteria Evaluation and Validation Scheme, an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.

**Confidentiality:** The prevention of unauthorized disclosure of information.

**Deliverables List:** A document produced by a CCTL containing the definition of the documents comprising the security target, all representations of the TOE, and developer support required to conduct an IT security evaluation in accordance with the laboratory's evaluation work plan.

**Evaluation:** The assessment of an IT product against the Common Criteria using the Common Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Methodology to determine if the profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

**Evaluation and Validation Scheme:** The systematic organization of the functions of evaluation and validation within a given country under the authority of a Validation Body in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved.

**Evaluation Schedule:** The schedule established by a CCTL for the conduct of an IT security evaluation.

**Evaluation Technical Report:** A report giving the details of the findings of an evaluation, submitted by the CCTL to the NIAP Validation Body as the principal basis for the validation report.

**Evaluation Work Plan:** A document produced by a CCTL detailing the organization, schedule, and planned activities for an IT security evaluation.

**Integrity:** The prevention of the unauthorized modification of information.

**Interpretation:** Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the Common Criteria and/or Common Methodology.

**IT Product:** A package of IT hardware, software, and/or firmware providing functionality designed for use or incorporation within a multiplicity of IT systems.

**IT System:** A group of IT products, either tightly or loosely coupled, working together in a specific configuration to provide a capability or system solution to a consumer in response to a stated need.

**IT Security Evaluation Criteria:** A compilation of the information which needs to be provided and actions which need to be taken in order to provide grounds for confidence that security evaluations will be carried out effectively and to a consistent standard.

**IT Security Evaluation Methodology:** A methodology which needs to be used by evaluation facilities in applying IT security evaluation criteria in order to give grounds for confidence that evaluations will be carried out effectively and to a consistent standard.

**National Voluntary Laboratory Accreditation Program (NVLAP):** The U.S. accreditation authority for CCTLs operating within the NIAP Common Criteria Evaluation and Validation Scheme.

**NIAP Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the Common Criteria Evaluation and Validation Scheme.

**Observation Reports:** A report issued to the NIAP Validation Body by a CCTL or sponsor identifying specific problems or issues related to the conduct of an IT security evaluation.

**Party:** A signatory to the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security*.

**Protection Profile:** An implementation independent set of security requirements for a category of IT products which meet specific consumer needs.

**Recognition of Common Criteria Certificates:** With respect to the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security*, acknowledgment by one Party of the validity of the Common Criteria certificates issued by another Party.

**Scope of Accreditation:** The NIAP-approved test methods for which a CCTL has been accredited by NVLAP.

**Security Target:** A specification of the security required (both functionality and assurance) in a Target of Evaluation (TOE), used as a baseline for evaluation under the Common Criteria. The security target specifies the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed.

**Shadow Evaluations:** The placement of technical personnel in selected CCTLs by the NIAP Validation Body for the express purpose of observing and/or participating in Common Criteria-based evaluations in a variety of information technology areas.

**Sponsor:** The person or organization that requests a security evaluation of an IT product or protection profile.

**Target of Evaluation (TOE):** An IT product or group of IT products configured as an IT system and associated documentation that is the subject of a security evaluation under the Common



Criteria. Also, a protection profile that is the subject of a security evaluation under the Common Criteria.

**Test Method:** An evaluation assurance package from the Common Criteria and the associated evaluation methodology for that assurance package from the Common Methodology.

**Validation:** The process carried out by the NIAP Validation Body leading to the issue of a Common Criteria certificate.

**Validated Products List:** A publicly available document issued periodically by the NIAP Validation Body giving brief particulars of every IT product or protection profile which holds a currently valid Common Criteria certificate awarded by that body and every product or profile validated or certified under the authority of another Party for which the certificate has been recognized.

**Validation Report:** A publicly available document issued by the NIAP Validation Body which summarizes the results of an evaluation and confirms the overall results, (i.e., that the evaluation has been properly carried out, that the Common Criteria, the Common Methodology, and scheme-specific procedures have been correctly applied and that the conclusions of the evaluation technical report are consistent with the evidence adduced).

## **Annex B. Requirements for Validation Body**

The following requirements for the NIAP Validation Body have been derived from a variety of sources including ISO/IEC Guide 65 [ISO96], General Requirements for Bodies Operating Product Certification Systems and the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security*. Additional information on the operation of the Validation Body can be found in Scheme Publication #2, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Validation Body Standard Operating Procedures*.

### ***General Requirements***

The NIAP Validation Body shall be impartial and the procedures under which it operates shall be administered in a non-discriminatory manner. In particular, the Validation Body shall have permanent staff responsible to NIST and NSA management. Day-to-day operations shall be carried out in a manner free from undue influence or control by anyone having a direct commercial interest in the evaluation and validation processes.

The Validation Body shall have and make available upon request:

- a) a chart showing the responsibility and reporting structure of the organization;
- b) a description of the means by which the organization obtains financial support;
- c) documentation describing its evaluation and validation scheme;
- d) documentation clearly identifying its legal status.

### ***Personnel***

The personnel of the Validation Body shall be competent and impartial for the functions they undertake.

Information on the relevant qualifications, training and experience of each member of staff shall be maintained by the Validation Body and kept up-to-date.

Personnel shall have available to them, clear, up-to-date, documented instructions pertaining to their duties and responsibilities.

If work is contracted to an outside body, the Validation Body shall ensure that the personnel carrying out the contracted work meet the applicable requirements of this Annex.

### ***Documentation and Change Control***

The Validation Body shall maintain a system for the control of all documentation relating to its evaluation and validation scheme and shall ensure that:

- a) current issues of the appropriate documentation are available at all relevant locations;
- b) documents are not amended or superseded without proper authorization;
- c) changes are promulgated in such a way that those who need to know are promptly informed and are in a position to take prompt and effective action;

- d) superseded documents are removed from use throughout the organization and its agencies;
- e) those with a direct interest in the scheme are informed of changes.

### ***Records***

The Validation Body shall maintain a record system to suit its particular circumstances and to comply with relevant regulations applied in its jurisdiction. The system shall include all records and other papers produced in connection with each validation; it shall be sufficiently complete to enable the course of each validation to be traced. All records shall be securely stored for a period of at least five years.

### ***Confidentiality***

The Validation Body shall have adequate arrangements to ensure confidentiality of the information obtained in the course of its validation activities at all levels of the organization. Client record confidentiality shall be maintained unless otherwise required by law.

### ***Quality Manual***

The Validation Body shall have a quality manual and documentation establishing the procedures by which it complies with the requirements of this Annex. These shall include as a minimum:

- a) a policy statement on the maintenance of quality;
- b) a brief description of the legal status of the Validation Body;
- c) the names, qualifications and duties of the personnel associated with the Validation Body;
- d) details of training arrangements for validation personnel;
- e) an organization chart showing lines of authority, responsibility, and allocation of functions within the Validation Body;
- f) details of procedures for monitoring IT product and protection profile evaluations;
- g) details of procedures for preventing the misuse of Common Criteria certificates and mutual recognition/service marks;
- h) the identities of any contractors and details of the documented procedures for assessing and monitoring their competence;
- i) details of any procedures for appeals or conciliation.

### ***Technical Oversight and Validation Procedures***

The Validation Body shall have the required facilities and procedures to carry out its technical oversight and validation responsibilities in accordance with the requirements of the scheme.

The Validation Body shall ensure that CCTLs conform to requirements established by the scheme and any additional requirements specified in the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security*.

The Validation Body shall draw up for each CCTL, a properly documented agreement covering all relevant procedures relating to evaluation including arrangements for ensuring confidentiality.

### ***Disputes***

The Validation Body shall have procedures to address disputes among the participants in the scheme. These procedures will be detailed in Scheme Publication #2, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Validation Body Standard Operating Procedures*.

### ***Periodic Assessments***

The Validation Body shall undertake periodic reviews of its compliance with the requirements of this Annex.

### ***Publications***

The Validation Body shall produce and update as necessary a validated products list. Each IT product or protection profile mentioned in the list shall be clearly identified. The list shall be available to the public.

A description of the evaluation and validation scheme shall be available in published form.

Copies of all scheme publications and other important information regarding the Validation Body shall be available on the NIAP web site at <http://niap.nist.gov>.

### ***Misuse of Common Criteria Certificates or Marks***

The Validation Body shall exercise proper control over the use of its Common Criteria certificates and associated service/mutual recognition marks.

It is incumbent upon the Validation Body to take whatever administrative, procedural, or legal steps necessary to prevent or counter the misuse of Common Criteria certificates or associated service/mutual recognition marks and to correct any false, misleading or improper statements regarding certificates, marks, or the evaluation and validation scheme.

### ***Withdrawal of Common Criteria Certificates***

The Validation Body shall have documented procedures for withdrawal of Common Criteria certificates and advertise the withdrawal in the next issue of the NIAP Validated Products List.

## Annex C. Requirements for Testing Laboratories

To become a CCTL, a testing laboratory must go through a series of steps which involve both the NIAP Validation Body and NVLAP. Accreditation by NVLAP is the primary requirement for achieving CCTL status. Scheme requirements which cannot be satisfied by NVLAP accreditation, are addressed by the NIAP Validation Body. A testing laboratory becomes a CCTL when the laboratory is approved by the Validation Body and is listed on the NIAP Approved Laboratories List.

### ***Laboratory Accreditation***

NVLAP is an activity for accrediting testing laboratories for competence to perform specific tests. Competence is defined as the ability of a laboratory to meet the NVLAP conditions and to conform to the criteria in NVLAP publications for test methods. The process administered by NVLAP:

- a) provides the technical and administrative mechanisms for national and international recognition for competent laboratories based on a comprehensive procedure for promoting confidence in testing laboratories that show that they operate in accordance with NVLAP's requirements;<sup>19</sup>
- b) provides laboratory management with documentation for use in the development and implementation of their quality systems;
- c) identifies competent laboratories for use by regulatory agencies, purchasing authorities, and product certification systems;
- d) provides laboratories with guidance from technical experts to aid them in reaching a higher level of performance, resulting in the generation of improved engineering and product information; and
- e) promotes the acceptance of test results between countries, and facilitates cooperation between laboratories and other bodies to assist in the exchange of information and experience, facilitating removal of non-tariff barriers to trade and promoting the harmonization of standards and procedures.

NVLAP is composed of a series of laboratory accreditation programs (LAPs) which are established on the basis of requests and demonstrated need.<sup>20</sup> The specific test methods, types of test methods, products, services, or standards to be included in a LAP are determined by an open process during the establishment of the LAP. NVLAP accreditation is:

- a) based on evaluation of a laboratory's technical qualifications and competence for conducting specific test methods, measurements and services in specified field of testing;
- b) granted only after thorough evaluation of the applicant has demonstrated that all NVLAP criteria have been met;

---

<sup>19</sup> NVLAP operates under a Quality Management System to ensure that the NVLAP program meets the requirements of the U.S. Code of Federal Regulations (as augmented), and the various international standards for laboratory accreditation and quality management.

<sup>20</sup> Based on the need to develop a security testing industry within the U.S. and to provide for qualified laboratories to participate in the Common Criteria Scheme, NIAP requested that NVLAP establish a new LAP specifically for IT security testing.

- c) acknowledged by the issuance of two documents to attest to that compliance: (1) a Certificate of Accreditation, and (2) a Scope of Accreditation which details the specific test methods, measurements and services for which a laboratory has been accredited;
- d) administered in a nondiscriminatory manner;
- e) not conditional on the size of the laboratory or on its membership in any association or group;
- f) based on assessing the competence of the laboratory against all of the NVLAP requirements.

NVLAP assessment for laboratory accreditation will include a variety of activities. During the assessment, a testing laboratory demonstrates compliance with general technical and methodological criteria to conduct security evaluations of IT products according to:

- a) ISO/IEC Guide 25, *General Requirements for the Competence of Calibration and Testing Laboratories*;
- b) NIST Handbook 150, *Procedures and General Requirements*;
- c) NIST Handbook 150-20, *Information Technology Security Testing—Common Criteria*.

The NVLAP assessment includes a series of proficiency tests covering the fundamentals of Common Criteria, Common Methodology, computer science, computer security, information technologies, and the demonstration of applied evaluation skills. These proficiency tests are tailored by NVLAP to the laboratory's accreditation request and proposed scope of accreditation, (i.e., focusing on the specific tests methods for which the laboratory is seeking accreditation).

The purpose of the proficiency tests is to demonstrate the laboratory's competence in applying the Common Criteria and the Common Methodology to security evaluations of IT products. The tests allow NVLAP to observe the laboratory in operation and provide an opportunity for the laboratory to demonstrate its competence in conducting evaluations.

As part of its proficiency testing, NVLAP will use, whenever possible, reference implementations of IT products to assess a laboratory's applied evaluation skills. These reference implementations are intended to exercise the specific test method or test methods being requested by the laboratory in its proposed scope of accreditation. Reference implementations provide a measure of standardization in the proficiency tests administered to laboratories seeking to become CCTLs and serve to promote consistency of testing across all laboratories in the scheme. NVLAP will use the results of its observations to complete its assessment of the testing laboratory.

The steps to becoming accredited are summarized below. Testing laboratories must:

- a) apply to NVLAP for laboratory accreditation specifying proposed scope of accreditation (i.e., the test methods it intends to use in conducting IT security evaluations);<sup>21</sup>
- b) be assessed by NVLAP for general technical and methodological competence in designated areas and for specific IT security evaluation competence to include demonstrating the laboratory's capability to apply selected test methods;
- c) receive NVLAP accreditation for selected scope of test methods.

---

<sup>21</sup> Test methods are selected from a NIAP Approved Test Methods List, maintained by the Validation Body. These test methods are derived from Common Criteria evaluation assurance packages, (e.g., pre-defined evaluation assurance levels), and the associated evaluation methodology from the Common Methodology.

A testing laboratory wishing to expand the scope of its accreditation, must take the following steps:

- a) select the new test method or test methods the laboratory intends to add to its expanded scope of accreditation;
- b) be assessed by NVLAP for specific IT security evaluation competence in areas covered by the expanded scope of accreditation;
- c) receive NVLAP accreditation for expanded scope of test methods.

### ***Becoming a Common Criteria Testing Laboratory***

A testing laboratory interested in becoming a CCTL must:

- a) receive NVLAP accreditation for the appropriate scope of test methods;
- b) satisfy NIAP Common Criteria Scheme-specific requirements.

At present, there are only three scheme-specific requirements imposed by the Validation Body. NIAP approved CCTLs:

- a) must reside within the U.S. and be a legal entity, duly organized and incorporated, validly existing, and in good standing under the laws of the state where the laboratory intends to do business;<sup>22</sup>
- b) must agree to accept U.S. Government technical oversight and validation of evaluation-related activities in accordance with the policies and procedures established by the NIAP Common Criteria Scheme (see Chapter 5);
- c) must agree to accept U.S. Government participants in selected Common Criteria evaluations conducted by the laboratory in accordance with the policies and procedures established by the NIAP Common Criteria Scheme (see Chapter 3.2).

To avoid unnecessary expense and delay in becoming a NIAP-approved testing laboratory, it is strongly recommended that prospective CCTLs ensure that they are able to satisfy the scheme-specific requirements prior to seeking accreditation from NVLAP. This can be accomplished by sending a letter of intent to the NIAP Validation Body prior to entering the NVLAP process. A sample letter of intent is provided in Annex H.

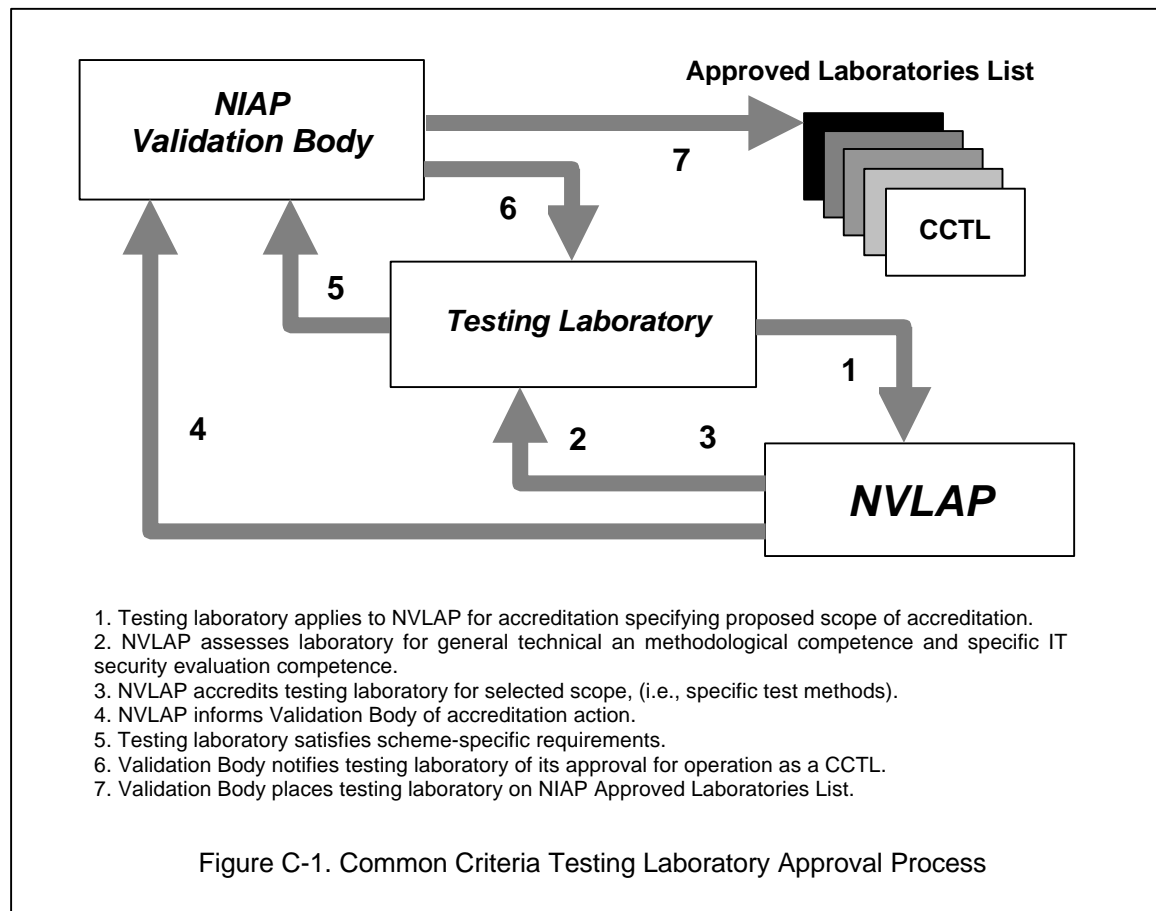
The NIAP Validation Body reserves the right to levy additional scheme-specific requirements (either technical or administrative), as necessary, when deemed to be in the best interest of the U.S. Government and overall evaluation and validation effort.

Once NVLAP accreditation is received and all additional scheme-specific requirements are met, the testing laboratory is designated a CCTL by the NIAP Validation Body and placed on the NIAP Approved Laboratories List. Listing on the approved laboratories list enables the CCTL to conduct IT security evaluations within the scope of its NVLAP accreditation.

---

<sup>22</sup> Assuming all other U.S. laws and regulatory requirements have been met, a foreign-owned enterprise could establish a testing laboratory in the U.S., become accredited under NVLAP, and be approved by NIAP as a CCTL. However, in order to meet the letter and spirit of the NIAP Common Criteria Scheme requirements, a foreign-owned laboratory must maintain a substantial presence within the U.S., (i.e., a demonstrated, fully operational security testing capability).

Figure C-1 illustrates the general process of becoming an approved CCTL on the NIAP Approved Laboratories List. The numbers in the figure are keyed to the legend and represent the particular steps in the process.



### ***Maintaining CCTL Status***

To maintain its status as a NIAP-approved testing laboratory, a CCTL must ensure that its NVLAP accreditation remains current. CCTLs must be re-accredited every two years in accordance with NIST Handbook 150-20, *Information Technology Security Testing—Common Criteria*. Failing to retain NVLAP accreditation will result in withdrawal of the CCTL from the NIAP Approved Laboratories List.



## **Annex D. Responsibilities of Evaluation Sponsors**

This annex contains information regarding the responsibilities of an IT security evaluation sponsor. In many cases, the sponsor of an evaluation will be the product developer. If the developer and sponsor are separate entities and the sponsor is relying on the developer to meet selected obligations contained in this annex, the sponsor must ensure that those obligations are covered by an appropriate contractual vehicle. Some of the items listed below will be applicable to IT product evaluations only and not to the evaluation of protection profiles. Additional sponsor-related information can be found in Scheme Publication #5 *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Guidance to Sponsors of Evaluations*.

### ***Sponsor Responsibilities prior to Evaluation***

During the period preceding the actual security evaluation, it is the responsibility of the sponsor:

- a) to determine the security target for the evaluation and any protection profiles which the security target will attempt to satisfy;
- b) to secure all legal rights to the Target of Evaluation (TOE) and other deliverables necessary to conduct the evaluation and to indemnify the CCTL and Validation Body in this area;
- c) to provide to the Validation Body, written confirmation of the nature and extent of proprietary information associated with the TOE;
- d) to obtain the written consent of the IT product developer regarding the conditions for limiting access to proprietary information associated with the TOE;
- e) to ensure that the CCTL submits and gains acceptance of the evaluation into the scheme;
- f) to ensure that the CCTL submits a copy of all required documentation to the Validation Body;
- g) to meet all requests from the Validation Body for information and support during evaluation and validation;
- h) to give permission for the future release of evaluation results including extracts from evaluation technical reports that are relevant to Common Criteria certificate maintenance activities;
- i) to state whether the TOE's Common Criteria certificate is to be maintained under the Certificate Maintenance Program, and if so, to specify in the security target and assurance maintenance plan, the requirements for re-evaluation and maintenance of the certificate;
- j) to agree not to make any statements in press releases or any other promotional material which might misrepresent the conclusions of the evaluation and validation or might otherwise bring the scheme into disrepute;
- k) to attend meetings with the CCTL and the Validation Body, as required.

### ***Sponsor Responsibilities during Evaluation***

While the security evaluation is in progress, it is the responsibility of the sponsor:

- a) to inform the CCTL of any changes to the TOE which may affect the security evaluation;

- b) to answer any questions from the CCTL arising from the analysis of the security target, protection profile or other evaluation deliverables;
- c) to provide the CCTL and Validation Body with detailed proposals for resolving problems that arise during the course of evaluation;
- d) to provide the CCTL with a schedule for the delivery of all items necessary for the conduct of the evaluation as outlined in the deliverables list;
- e) to ensure the timely provision to the CCTL of identified deliverables for the evaluation including:
  - 1) the security target;
  - 2) any protection profiles which the security target will attempt to satisfy;
  - 3) the TOE in its various representations, (e.g., architectural design, detailed design and implementation, source code), as required in the Common Criteria;
  - 4) configuration data, defining all configurable options of the TOE which could affect security;
  - 5) evidence of security, (e.g., justifications, conformance analyses, proofs and test materials);
  - 6) development documentation describing configuration control, programming languages, compilers, and developer security;
  - 7) operational documentation for delivery, configuration, start-up, and operation;
  - 8) user and administrative documentation.
- f) to provide access to an appropriate facility where the TOE can be installed and tested in the evaluated configuration;
- g) to provide general support to evaluators and validation personnel, including training and access to the developers staff for technical discussions about the product;
- h) to hold evaluation progress reviews with the CCTL and Validation Body when required.

### ***Sponsor Responsibilities after Evaluation***

Upon completion of the security evaluation, it is the responsibility of the sponsor:

- a) to reach agreement with the Validation Body that the validation report fairly and accurately represents the security target and outcome of the evaluation;
- b) to accept the conclusions in the validation report;
- c) to inform the Validation Body of any factors that would invalidate or change the validation report;
- d) to reproduce and distribute the validation report only in its entirety;

- e) to advertise and market an IT product or protection profile as a validated product or profile only on the basis of a valid Common Criteria certificate;
- f) to provide the Validation Body reference material uniquely identifying the evaluated version of the TOE;
- g) to retain archival material returned from the CCTL for a period of five years;
- h) to ensure maintenance of the Common Criteria certificate by complying with the change control requirements specified in the security target, evaluation technical report, or validation report, for proposed changes to the TOE;
- i) to retain all evaluation deliverable change information and related test evidence for potential use in future evaluations.

## **Annex E. Common Criteria Certificates**

The following information shall be included on all Common Criteria certificates issued by the NIAP Validation Body. In addition to the information listed, the mutual recognition mark shall be placed on each Common Criteria certificate issued by the Validation Body. The certificate is only valid in conjunction with the full validation report produced for its associated IT product or protection profile evaluation.

### ***Certificates Associated with IT Product Evaluations***

A Common Criteria certificate issued by the Validation Body resulting from the validation of an IT product evaluation shall include the following information:

- a) Product developer;
- b) Product name;
- c) Version and release numbers;
- d) Protection profile identifier (if claiming conformance);
- e) Evaluation platform;
- f) Name of CCTL;
- g) Validation report number;
- h) Date issued;
- i) Assurance level;
- j) Signature of NIST and NSA certificate-issuing authorities;
- k) A statement indicating that:
  - 1) The IT product has been evaluated at an accredited testing laboratory using the Common Methodology for Information Technology Security Evaluation (version number) for conformance to the Common Criteria for Information Technology Security Evaluation (version number) as articulated in the product's functional and assurance security specification contained in its security target;
  - 2) The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence presented;
  - 3) The issuance of a certificate is not an endorsement of the IT product by NIST, NSA, or any agency of the U.S. Government and no warranty of the product is either expressed or implied;
  - 4) The certificate applies only to the specific version of the product in its evaluated configuration.

A sample product-related Common Criteria certificate is provided in Figure E-1.


	<p><i>National Information Assurance Partnership</i></p> <p><b>Common Criteria Certificate</b></p> <p><b>IT Product Developer</b></p>
<p>The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version X) for conformance to the Common Criteria for IT Security Evaluation (Version X). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.</p>	
Product Name:	Name of CCTL:
Version and Release Numbers:	Validation Report Number:
Protection Profile Identifiers:	Date Issued:
Evaluation Platform:	Assurance Level:
<hr/> Director, Information Technology Laboratory National Institute of Standards and Technology	<hr/> Deputy Director, Information Systems Security Organization, National Security Agency

Figure E-1. Sample Common Criteria Certificate for an IT Product


### ***Certificates Associated with Protection Profile Evaluations***

A Common Criteria certificate issued by the Validation Body resulting from the validation of a protection profile evaluation shall include the following information:

- a) Protection profile developer;
- b) Protection profile name/identifier;
- c) Version number;
- d) Functionality and assurance packages;
- e) Name of CCTL;
- f) Validation report number;
- g) Date issued;
- h) Signature of NIST and NSA certificate-issuing authorities;
- i) A statement indicating that:

- 1) The protection profile has been evaluated at an accredited testing laboratory using the Common Methodology for Information Technology Security Evaluation (version number) for conformance to the Common Criteria for Information Technology Security Evaluation (version number);
- 2) The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence presented;
- 3) The issuance of a certificate is not an endorsement of the protection profile by NIST, NSA, or any agency of the U.S. Government and no warranty of the profile is either expressed or implied;
- 4) The certificate applies only to the specific version of the protection profile as evaluated.

A sample profile-related Common Criteria certificate is provided in Figure E-2.

	<p><i>National Information Assurance Partnership</i>  <b>Common Criteria Certificate</b></p>
<p><b>Protection Profile Developer</b></p>	
<p>The protection profile identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version X) for conformance to the Common Criteria for IT Security Evaluation (Version X). This certificate applies only to the specific version of the protection profile as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the protection profile by any agency of the U.S. Government and no warranty of the protection profile is either expressed or implied.</p>	
<p>Protection Profile Name/Identifier:          Version Number:          Functionality Package:          Assurance Package:</p>	<p>Name of CCTL:          Validation Report Number:          Date Issued:</p>
<p>_____          Director, Information Technology Laboratory          National Institute of Standards and Technology</p>	<p>_____          Deputy Director, Information Systems Security          Organization, National Security Agency</p>
<p>Figure E-1. Sample Common Criteria Certificate for a Protection Profile</p>	

## Annex F. Certificate Maintenance

This annex addresses the issue of Common Criteria certificate maintenance and the associated activities necessary to participate in the *Certificate Maintenance Program (CMP)*. Additional information can be found in Scheme Publication #6 *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Certificate Maintenance Program*.

### Overview

The Common Criteria Scheme provides an opportunity for sponsors of security evaluations to maximize previous evaluation results and to cost-effectively continue to participate in the evaluation and validation processes over time. Certificate maintenance is an important issue that should be addressed by all scheme participants as early as possible in the evaluation life cycle. A significant amount of planning and preparation must occur on the part of the sponsor of the evaluation, product developer (if other than the sponsor), the CCTL, and the NIAP Validation Body.

Certificates are only valid for a specific version of a TOE. However, most IT products that have been evaluated, continue to change over time as the products evolve and are enhanced with new features and capabilities.<sup>23</sup> These changes are usually outside the scope of the current certificate issued by the Validation Body. The CMP provides a means of establishing confidence that the assurance in a TOE is maintained without always requiring a formal re-evaluation. The sponsor, under the CMP, is therefore able to maintain their TOE without incurring the costs associated with re-evaluating each change and at the same time, minimize the cost of future re-evaluation. In addition, the CMP has been designed to ensure that mutual recognition of certificates issued by the Validation Body is not jeopardized.

Versions of a TOE produced while in the CMP receive an updated Common Criteria certificate from the Validation Body provided all assurance maintenance requirements have been met. The Validation Body confirms that consumers or end users can have equal confidence in the product variant as they have in the initial, validated version of the TOE.

### The Assurance Maintenance Paradigm

Maintenance of assurance is a concept applied after a TOE has been evaluated against the Common Criteria and validated by the NIAP Validation Body. The maintenance of assurance requirements ensures the TOE will continue to meet its security target as changes are made to the IT product or its environment. Such changes include the discovery of new threats or vulnerabilities, changes in user requirements, the correction of errors found in the validated TOE, and other updates to the functionality provided.

The main goal of the Common Criteria assurance maintenance requirements is, therefore, to define a set of requirements which can be applied to provide confidence that the assurance established in a TOE is being maintained, without always requiring a complete, formal re-evaluation of new versions of the TOE. In some cases however, changes may be so significant that only a complete, formal re-evaluation can be relied upon to ensure that assurance has been maintained.

---

<sup>23</sup> While the assurance maintenance concepts in this annex are primarily applicable to IT product evaluations, many of those same concepts can be applied to protection profile evaluations. Additional guidance on assurance maintenance concepts for protection profile evaluations can be found in related scheme publications available from the NIAP Validation Body.

## ***Entering the Certificate Maintenance Program***

To support sponsor requirements for certificate maintenance, the Common Criteria Scheme has defined three phases comprising an *assurance maintenance cycle*:

- a) an *acceptance phase*, at the start of a cycle, in which the developer's plans and procedures for assurance maintenance during the cycle are established by the developer and independently evaluated by a CCTL and validated by the NIAP Validation Body;
- b) a *monitoring phase*, in which the developer provides at one or more points during the cycle, evidence that the assurance in the TOE is being maintained in accordance with the established plans and procedures, (this evidence being independently evaluated by a CCTL);
- c) a *re-evaluation phase*, completing the cycle, in which an updated version of the TOE is submitted to a CCTL for re-evaluation based on the changes affecting the TOE since the previously validated version.

The Common Criteria assurance maintenance requirements address primarily the first two of these phases, while providing support for the third.

A TOE can enter the monitoring phase only when the acceptance phase has been successfully concluded, (i.e., the developer's plans and procedures for assurance maintenance have been evaluated by a CCTL and approved by the Validation Body as part of the initial TOE evaluation). If the developer makes changes to these plans or procedures during the monitoring phase then the TOE will need to re-enter the acceptance phase to get the changes accepted.

During the monitoring phase, the developer follows the assurance maintenance plans and procedures, conducting an analysis of the security impact of changes affecting the TOE (*security impact analysis*). At selected points during this phase, a CCTL independently checks (by means of an evaluation) the developer's work. The developer is required to ensure that the plans and procedures are followed, and that security impact analysis is performed correctly. Therefore, once a TOE is in the monitoring phase, it becomes possible to have confidence that the assurance in the TOE has been maintained for new versions of the TOE produced by the developer.

A TOE that is subject to change would not continue in the monitoring phase for an indefinite period. At some point, a re-evaluation of the TOE would be necessary. The decision as to when a re-evaluation would be required is dependent on cumulative changes to the TOE as well as especially significant changes. For example, a large number of minor changes could have an impact on assurance equivalent to that of a single major change. The developer's assurance maintenance plan defines the scope of the changes that may be made to the TOE during the monitoring phase. In a similar way, it would not be possible to increase the assurance level of a TOE during the monitoring phase. This could only be achieved by means of a formal re-evaluation of the TOE (making appropriate reuse of previous evaluation results).

The assurance maintenance status of the TOE must be reviewed if it is discovered that the assurance maintenance procedures are not being followed, and that as a result, assurance in the TOE is undermined. In some cases, the developer may be required to submit the TOE for re-evaluation, and afterwards start a new assurance maintenance cycle.

### **TOE Acceptance**

A sponsor can only request entry into the CMP at the start of an IT security evaluation. If the maintenance approach is selected over the full re-evaluation approach, the security target must include the assurance maintenance requirements as a statement of commitment to the certificate maintenance process. A completed evaluation must have resulted in the award of a Common



Criteria certificate from the NIAP Validation Body stating that the assurance requirements in the security target have been met.

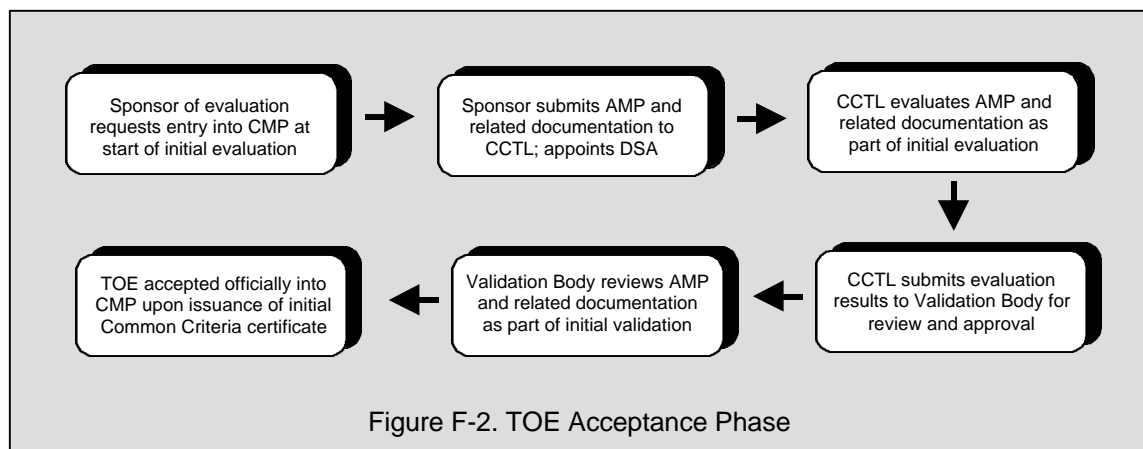
During the TOE acceptance phase, the Common Criteria assurance maintenance requirements focus on the Assurance Maintenance Plan (AMP) and the TOE component categorization report. Formal application to the CMP commences with the sponsor's submission of an AMP and a TOE component categorization report to a CCTL for evaluation.<sup>24</sup> The CCTL is normally the testing laboratory conducting the initial evaluation of the TOE, although a different CCTL may be selected by the sponsor to carry out CMP-related activities. The NIAP Validation Body must approve the AMP and TOE component categorization report as part of the initial validation process.

The sponsor of the evaluation must also appoint a Developer Security Analyst (DSA), who has the primary responsibility for ensuring that the assurance of the TOE is maintained while the product is in the CMP. The DSA should be familiar with the TOE, the results of the initial evaluation, and all relevant scheme documents. It is advisable for the sponsor to appoint a DSA during the initial evaluation, if possible, to ensure continuity throughout the evaluation and validation process.

In summary, a sponsor of an evaluation can participate in the CMP once the following conditions have been met:

- a) the TOE and its associated assurance maintenance requirements, (i.e., the AMP and TOE component categorization report) have been evaluated by a CCTL and validated by the NIAP Validation Body;
- b) a DSA has been appointed for the TOE.

The sponsor can remain in the CMP provided that the AMP and the general rules of the scheme are followed. Modifications to AMPs are permitted only with the concurrence of the Validation Body. Figure F-2 illustrates the activities associated with the TOE acceptance phase.



<sup>24</sup> The specific requirements for the Assurance Maintenance Plan and TOE component categorization report, as well as all other assurance maintenance requirements, are described in Part 3 of the Common Criteria.

## TOE Monitoring

The TOE monitoring phase begins with the sponsor's submission to the Validation Body proposed changes to the IT product. The Validation Body assigns a validator to the product for the monitoring of CMP activities, reviews the proposed changes, and verifies that the changes are within the scope of the approved AMP and TOE component categorization report. If the proposed changes are within scope, the Validation Body gives the sponsor authorization to proceed. Upon receiving authorization to proceed, the sponsor selects a CCTL to conduct CMP evaluation maintenance activities (in cooperation with the product developer).

The selected CCTL functions primarily in an evaluation and auditing role during the TOE monitoring phase. The sponsor of the evaluation is required to provide evidence to the CCTL (from the product developer) demonstrating that the assurance of the TOE is being maintained. In addition to the AMP and TOE component categorization report, the primary evaluation maintenance input document is the security impact analysis. The developer's security impact analysis is based on the TOE component categorization report and is intended to provide confidence that assurance has been maintained in the TOE (through a comprehensive assessment of the security impact of all changes affecting the TOE since it was validated). The security impact analysis must provide appropriate justification (supported by evidence) as to why the assurance that the TOE meets in its security target is maintained. The CCTL audits the assurance maintenance process by assessing whether the developer is following the AMP and by evaluating the developer's security impact analysis for correctness and completeness. The CCTL also performs other testing as appropriate.

Site visits to the product developer should be undertaken by the CCTL in accordance with the AMP.<sup>25</sup> The frequency of the visits will be at the discretion of the CCTL but should occur at such intervals as to establish confidence on the part of the CCTL that the DSA is following the AMP and the requirements outlined in the CMP. The CCTL reports the results of their evaluation maintenance activities to the Validation Body in a Certificate Maintenance Report (CMR) in accordance with the requirements outlined in Scheme Publication #6 *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Certificate Maintenance Program*. The CMR is reviewed by the Validation Body and a new Common Criteria certificate is issued for the IT product (with appropriate version or release numbers indicated) if:

- a) the security impact analysis shows that changes to the TOE are within the scope of the CMP approval; and
- b) there are no outstanding non-compliances with the AMP or CMP, in general.<sup>26</sup>

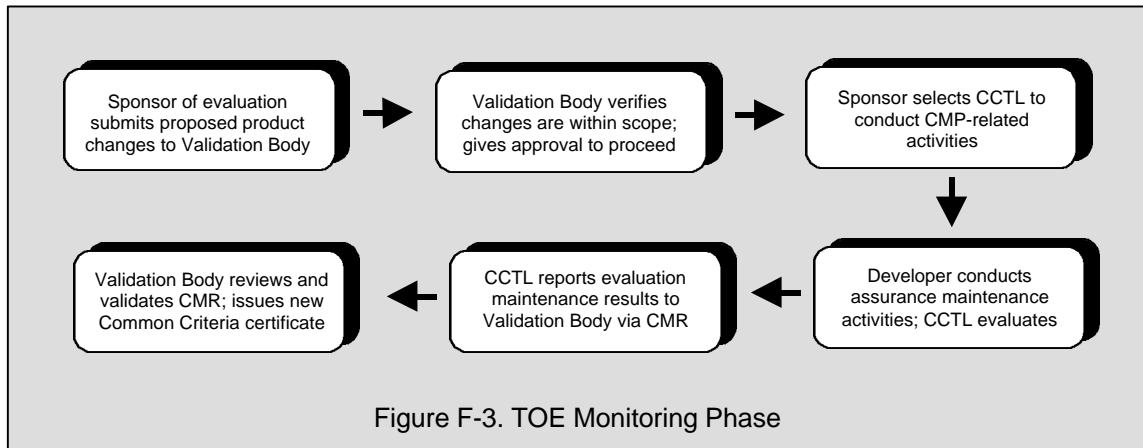
The sponsor is required to submit an annual Certificate Maintenance Summary Report (CMSR) to the Validation Body providing a summary of all certificate maintenance activities conducted during the previous year. The report, submitted while the product remains in the CMP, gives the Validation Body important information with which to gauge the continued validity of the AMP. The requirements for the annual CMSR are described in Scheme Publication #6 *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Certificate Maintenance Program*.

---

<sup>25</sup> The Validation Body may also conduct developer and CCTL site visits, as appropriate, to audit the CMP activities being carried out within the scheme.

<sup>26</sup> The Common Criteria certificate issued by the Validation Body from the initial evaluation will indicate that the IT product is officially in the CMP. The Evaluation Assurance Level (EAL) obtained during that evaluation will be noted with a reference to the augmentation for the assurance maintenance requirements.

Figure F-3 illustrates the activities associated with the CMP TOE monitoring phase.



### TOE Re-evaluation

The third phase of the assurance maintenance cycle is the re-evaluation phase, in which the selected CCTL makes use of the developer's documentation and assurance maintenance evidence to re-examine parts of the TOE, using the assurance components applicable for the target assurance level. A CMP re-evaluation addresses changes to the IT product and/or its security target since the most recent evaluation of the TOE. Re-evaluation activities would be scheduled in the AMP, or could be required in response to unforeseen significant changes to the TOE and/or its environment for which assurance maintenance activities were considered inappropriate.

### ***Selection of CCTL for Maintenance Activities***

The sponsor has considerable flexibility in selecting CCTLs for the initial evaluation, CMP-related activities, and ultimately for the re-evaluation of the TOE. Each activity can be performed by a different CCTL, the same CCTL, or any combination thereof, subject to the conditions stated above. Sponsors participating in the CMP must ensure that appropriate deliverables are made available to any CCTL. As in the case of the initial evaluation, a CCTL providing consultancy services to a sponsor or product developer (if other than the sponsor) must ensure that its independence is not compromised if the CCTL is also contracted to carry out the review, audit or re-evaluation activities as part of the CMP.

## **Annex G. Demonstrating Common Criteria Conformance**

Sponsors of security evaluations can participate in many different types of activities when considering the issue of IT product or protection profile conformance to Common Criteria requirements. While all of these activities are recognized as legitimate for certain constituencies or communities of interest, some are outside the scope of the Common Criteria Scheme as described in this document and will not result in the issuance of a Common Criteria certificate. The different approaches to conformance (both within the scope of the scheme and outside the scope of the scheme) are summarized below and illustrated pictorially in Figure G-1.

### ***Conformance Demonstrated by Third Party Evaluation and U.S. Government Validation***

(NIAP Common Criteria Scheme)

A sponsor can submit an IT product or protection profile to a NVLAP-accredited CCTL for a formal, independent, third party evaluation with government-sponsored validation. The sponsor asserts conformance to Common Criteria requirements based on the results of the security evaluation conducted by the CCTL and the validation process conducted by the NIAP Validation Body. A final report is published by the NIAP Validation Body and a Common Criteria certificate is issued for the product or profile after successfully completing evaluation and validation. Following validation, the IT product or protection profile is placed on the NIAP Validated Products List. Sponsors employing this approach will receive the benefits that accrue from the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security*.

### ***Conformance Demonstrated by Developer Self Declaration***

(Outside Scope of NIAP Common Criteria Scheme)

An IT product or protection profile developer can assert that their product or profile has been built to meet the requirements articulated in the Common Criteria. The developer sells the product or profile to the consumer without the intervention of any third party security testing or evaluation activity. This approach provides a degree of assurance that may be acceptable to certain constituencies or consumers. Developer self declaration of conformity is outside the scope of the scheme, and thus, involves no formal government validation process. Developers employing this approach will not be able to have their IT products or protection profiles placed on the NIAP Validated Products List and will not receive the benefits that accrue from the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security*.

### ***Conformance Demonstrated by Third Party Evaluation***

(Outside Scope of NIAP Common Criteria Scheme)

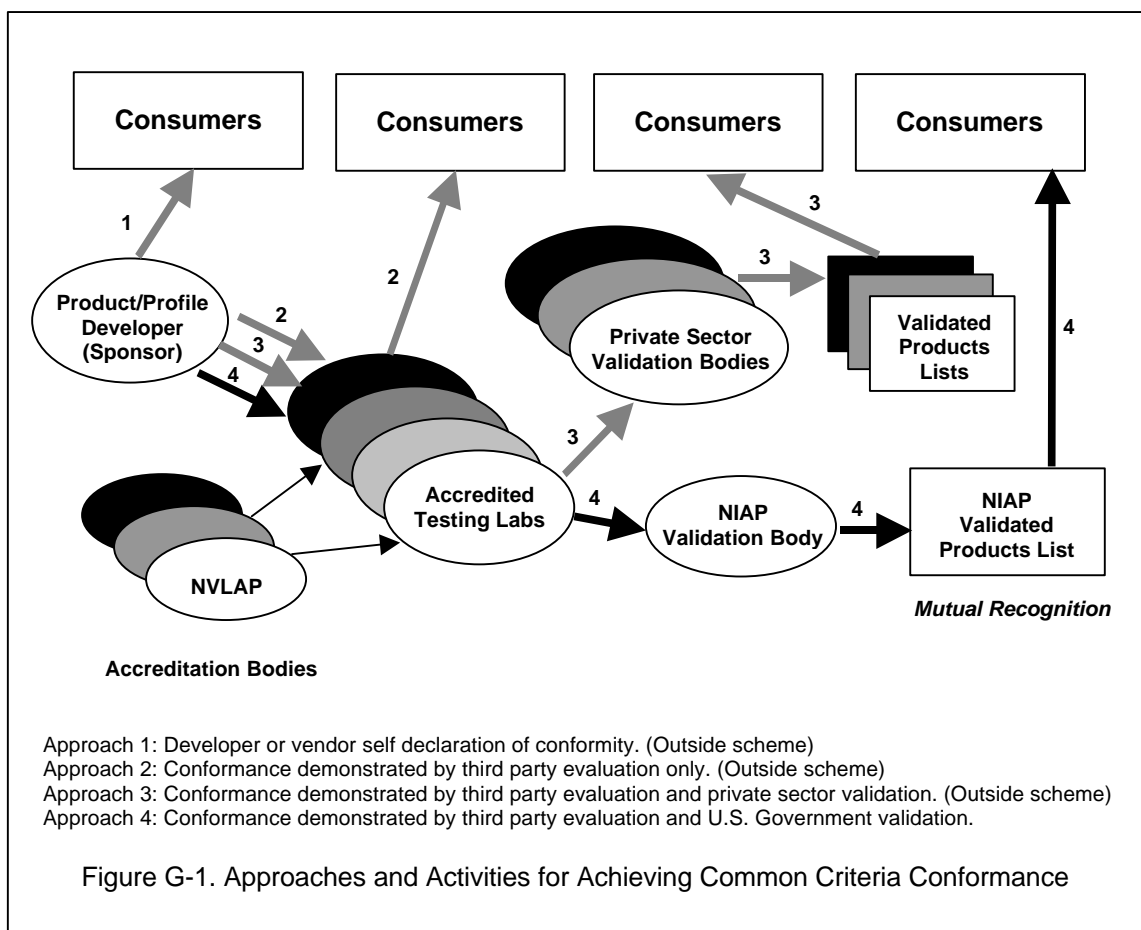
A sponsor can submit an IT product or protection profile to a NVLAP-accredited CCTL for a formal, independent, third party evaluation without validation. The sponsor asserts conformance to Common Criteria requirements based solely on the results of the security evaluation as articulated in the evaluation technical report produced by the CCTL. As in developer self declaration, conformance demonstrated by third party evaluation only without government or private sector validation, provides a degree of assurance that may be acceptable to certain constituencies or consumers. However, it is once again outside the scope of the scheme. Sponsors employing this approach will not be able to have their evaluated IT products or protection profiles placed on the NIAP Validated Products List and will not receive the benefits that accrue from the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security*.

## Conformance Demonstrated by Third Party Evaluation and Private Sector Validation

(Outside Scope of NIAP Common Criteria Scheme)

A sponsor can submit an IT product or protection profile to a NVLAP-accredited CCTL for a formal, independent, third party evaluation with private sector validation. This approach will likely be used by sponsors who wish to have their products or profiles evaluated by an accredited testing laboratory but are not interested in participating in a government-sponsored validation process. The sponsor is, however, interested in submitting the results of the security evaluation to a specific private sector validation body operating on behalf of a particular constituency or community of interest, (e.g., a banking association, a health care association, an industry consortium, or a trade association). A certificate may be issued by the validation body which provides recognition within that particular constituency or community of interest. There may also be validated products lists maintained by these private sector validation bodies as a service to their respective communities. Sponsors employing this approach will not be able to have their evaluated IT products or protection profiles placed on the NIAP Validated Products List and will not receive the benefits that accrue from the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security*.

Figure G-1 illustrates the different types of Common Criteria conformance activities and approaches that IT product and protection profile developers of can take according to consumer needs.



## Annex H. Letter of Intent

This annex provides a sample letter of intent that may be used by prospective CCTLs to convey necessary administrative information to the NIAP Validation Body. This information will be used by the Validation Body to determine if the prospective CCTL has satisfied the scheme-specific requirements as articulated in Annex C.

### Company Letter Head

Date

Director  
Common Criteria Evaluation and Validation Scheme  
National Information Assurance Partnership  
National Institute of Standards and Technology  
100 Bureau Drive, Mailstop 8930  
Gaithersburg, MD 20899-8930

This letter is formal notice that **COMPANY NAME** desires to participate as an approved laboratory in the National Information Assurance Partnership's (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS). **COMPANY NAME** recognizes that it must comply with both the requirements of the National Voluntary Laboratory Accreditation Program (NVLAP) for Information Technology Security Testing-Common Criteria Testing (NIST Handbooks 150 and 150-20) and the requirements of the NIAP CCEVS.

**COMPANY NAME** hereby acknowledges there are requirements for participation within the CCEVS dictated by the scheme in addition to the NVLAP requirements. In order to be placed on the NIAP Approved Laboratory List, **COMPANY NAME** acknowledges it must be accredited by NVLAP and comply with all of the requirements outlined in Scheme Publication #1, *NIAP CCEVS Organization, Management and Concept of Operations*; in particular the requirements of Sections 3.2 (placement of NIAP personnel in CCTLs), 3.3 (CCTL Requirements), and 5 (Technical Oversight and Validation).

**COMPANY NAME**, as of the date of this letter, is a legal entity, duly organized and incorporated, validly existing, and in good standing under the laws of the State of **STATE NAME** whose principal place of business is **CITY, STATE**.

Point of contact for this application is **POC NAME, TITLE, PHONE, E-MAIL ADDRESS**.

Sincerely,

**NAME**  
**TITLE**